

## 明細書

## 端末及び通信システム

## 技術分野

- 5      本発明は、ネットワークに接続された端末、該端末に関する通信制御方法及び該端末の制御プログラムに関する。特に、移動体端末装置、移動通信制御方法、および、移動端末の制御プログラムに関する。中でも、モバイルIP (Mobile IP) プロトコルを適用した移動通信システムにおける移動体端末装置に関する。

10

## 背景技術

近年移動体通信網のIP (Internet Protocol) 化の検討が活発化している。

- 15      IETF (Internet Engineering Task Force) は、Mobile IPv6仕様の標準化をすすめている (例えば、非特許文献1: Mobility Support in IPv6 <draft-ietf-mobileip-ipv6-24.txt>、Work in Progress 参照。 ) 。

- 20      Mobile IPv6の網構成要素は、移動ノード (MN: Mobile Node)、ホームエージェント (HA: Home Agent)、通信相手 (CN: Correspondent Node) である。

MNには、移動しても変わることのない一意のIPアドレス (ホームアドレス) が付与される。ホームアドレスと同じプレフィックスを持つリンクをホームリンクと呼ぶ。ここで、プレフィックスとは、IPアドレスのネットワーク部を示す。

- 25      MNはホームリンク以外のリンクに移動すると (移動先のリンクを在圏リンクという)、在圏リンクにおいてIPアドレスを取得す

る。このアドレスを気付アドレス (Care of Address、以下CoA  
で表す) とよぶ。MNは在圏リンクに移動した際に、在圏リンクに  
存在するルータが定期的に送信するルータ広告を受信する。MN  
はこのルータ広告に含まれるホームアドレスと異なるプレフィ  
5 ックスを検出することでホームリンクから在圏リンクへの移動  
を検知する。ルータ広告メッセージは、IPv6の近隣探索(Neighbor  
Discovery) (IETF RFC2461) において規定される。上記メッセ  
ージは、ルータが自分の存在を同一リンク上の他のノードに通知  
するために利用する。

- 10 MNは移動を検知すると、HAに位置登録を行う。位置登録信号及  
びその応答信号は、IPsecを用いてセキュリティを確保する。HA  
は、Binding Cacheにホームリンク以外に存在するMNのホームア  
ドレスと気付アドレスの対応情報 (バインディング情報) を保持  
する。次に、HAは、CNからMNのホームアドレス宛に送信されるパ  
15 ケットを捕捉するため、Gratuitous Neighbor Advertisementを  
マルチキャストして上記MNのプロキシとして動作する。

以下、CNがMN宛にパケットを送信する手順を説明する。

- CNはMNのホームアドレス宛にパケットを送信する。HAは上記  
MNのホームアドレス宛パケットを捕捉する。HAはBinding Cache  
20 を検索して、MNのホームアドレスに対応するCoAを取得する。HA  
は受信したパケットに該当CoA宛のIPヘッダを付加 (カプセル化  
) してパケットを送信する。HA-MNのカプセル化区間をモバイルト  
ンネルと呼ぶ。

- MNは上記CoA宛のパケットを受信すると、先に付加されたIPヘッダを  
25 除去 (デカプセル化) してオリジナルパケットを復元する。モバイルトン  
ネルは、IPsecによりセキュリティを確保してもよい。カプセル化パケット

を受信した MN は、CN に MN のバインディング情報を通知し、経路最適化を行ってもよい。

また、Mobile IPv6 をベースに局所的な移動管理を行う技術として、Hierarchical Mobile IPv6 mobility management (HMIPv6) が提案されている（非特許文献 2：Hierarchical Mobile IPv6 mobility management (HMIPv6) <draft-ietf-mobileip-hmipv6-07.txt>、Work in Progress 参照。）。

HMIPv6 は、HA と MN の間に MAP (Mobile Anchor Point) を備える。MAP は、ローカルな HA 機能を提供する。MAP は、配下に AR (Access Router) を備えてもよい。MN は、AR 又は MAP から MAP オプションを含むルータ広告を受信し、MAP の IP アドレスを取得する。MAP オプションには、MAP のグローバルアドレス、MAP のプレフィックス、MAP のプリファレンス、MAP までのホップ数等が含まれる。MAP は AR に以下のいずれかの方法により MAP オプションを通知する。

（1）MAP オプションを含むルータ広告をルータ（AR）に配信する。（2）MAP は IPv6 のルータリナンバリング機能を拡張して AR に MAP オプションを通知する。MAP が AR に MAP オプションを通知するかわりに、網管理者が AR に MAP オプションの情報を設定してもよい。

AR は、MAP オプションを含むルータ広告を受信すると、上記オプションを含むルータ広告を配下に位置する MN に対して送信する。

HMIPv6 対応 MN は MAP オプションを含むルータ広告を受信すると、MAP オプションの情報を格納する。HMIPv6 対応 MN は、MAP オプションに含まれる MAP プレフィックス（MAP が存在するリンク

のプレフィックス)と MN のインタフェース識別子から地域気付アドレス (Regional Core of Address : RCoA) を生成する。また、AR が送信するルータ広告に含まれるプレフィックス情報 (AR のプレフィックス) を用いて、HMIPv6 対応 MN はリンク気付アドレス (On-link CoA : LCoA) を生成する。LCoA は、Mobile IPv6 の気付アドレス (CoA) に相当する。

HMIPv6 対応 MN は、まず、MAP に位置登録を行う。MAP は、MN の RCoA と LCoA の対応情報を管理する。次に、MN は HA に位置登録を行う。HA は MN のホームアドレスと RCoA の対応情報を管理する。MN が MAP 内で移動した場合、MN は MAP の位置情報のみ更新する。

さらに、ノードの集合移動をサポートするモバイルルータを用いて、ネットワーク単位でモビリティを管理する Network Mobility 技術が注目されつつある (例えば、非特許文献 3 : "Network Mobility Support Goals and Requirements" <draft-ietf-nemo-requirements-01.txt>、Work in Progress 参照。)。モバイルルータは HA を持ち、HA に位置登録を行う。モバイルルータは、モバイル IP の MN 機能とルータ機能を備える。モバイルルータが移動する間のセッション連続性を維持するため、モバイルルータの HA とモバイルルータの間には、モバイル IP 技術を適用する。HA が、モバイルルータの配下に位置する端末宛のパケットを捕捉して、モバイルルータに転送する。このため、モバイルルータが移動する間のセッション連続性が維持できる。モバイルルータと HA の間のパケットには、IP ヘッダが付加される。モバイルルータを含む移動ネットワークは、固定ノード又は移動ノードを含む。移動ネットワーク内に移動ネットワークが存在してもよい。移動ネットワークのノードが移動ネットワーク外のノード

ドと通信する際、全トラフィックがモバイルルータとHA間のトンネルを通過する。

ある特定のマシン・アーキテクチャやハードウェア・プラットフォームをエミュレーションする技術に、仮想マシンがある。一般に、仮想マシンは、ソフトウェアで実現される。通常、仮想マシンはある装置の Operation System (OS) 上で動作する。このため、仮想マシンそのものを実行するために使われる OS をホスト OS と、仮想マシンの上で実行される OS をゲスト OS と呼ぶ。

一方、IP網におけるセッション制御プロトコルとして、  
10 SIP (Session Initiation Protocol) (非特許文献4: IETF RFC3261、SIP: Session Initiation Protocol参照。) が注目されている。SIPは、IETFで仕様化されたIPマルチメディア通信のセッション制御を行うプロトコルである。SIPを用いた代表サービスにVoIP (Voice over IP) がある。VoIPは音声情報をIPネットワーク上  
15 で送受信する技術である。SIPによるVoIP通信では、通信開始前に通信装置間に仮想的な通話路 (セッション) を設定する。IPパケット化された音声データは、設定した通信路上で転送される。VoIP通信においてSIPは、通信装置間のセッション確立、維持、切断を制御する。

20 さらに、セッション層でセキュリティ機能を提供するプロトコルとして、TLS (Transport Layer Security) (非特許文献5: IETF RFC2246、The TLS Protocol Version 1.0参照。) が注目されている。TLSは、トランスポート層とアプリケーション層の間に位置し、認証、暗号化を備えるセキュリティプロトコルである。TLS  
25 は、アプリケーション単位に実装される。

## 発明の開示

上記従来技術には、次のような課題があった。

- 領域Aと領域Bが相互接続され、領域Aに属する移動ノード (MN) が領域Bに移動した場合、領域Aに存在し、移動ノードの位置情報を保持するHAはMNのプロキシとして動作する。

Mobile IPv6は、移動しても変わることのない一意のIPアドレス (ホームアドレス) を移動ノードに付与することにより、移動ノードからのパケットに対してホームアドレスへの到達性を保証する。しかし、ユーザがMobile IPを利用するためには、移動ノードがMobile IPv6に対応する必要がある。また、移動ノード上で動作するアプリケーションがIPv6に対応する必要がある。しかし、現状では、Mobile IPv6に対応した移動ノードとIPv6に対応したアプリケーションが少ないという課題がある。

- また、VoIPサービスにおいて、音声情報の盗聴を防ぐため、音声パケットの暗号化が要求されている。図37は、Mobile IPv6対応移動ノードがVoIPサービスを利用する際のセキュリティ適用区間を示す。音声パケットに対するセキュリティは、移動ノード (MN1) と通信相手 (CN2) の間に適用される ((1) MN-CN間セキュリティ)。CN2は、MN1宛のパケット356にセキュリティ処理 (例えば、IPsec トランスポートモード) を施す。ここで、経路最適化前にMN1が送受信する音声パケットは、HA4を経由する。HA-MNのモバイルトンネルのセキュリティは、HA4とMN1の間に適用される ((2) MN-HA間セキュリティ)。モバイルトンネルにセキュリティを適用する場合、HAはオリジナルパケットにモバイルトンネル用のヘッダとIPsec用のヘッダ (357) を付加する。(1) MN-CN間セキュリティと (2) MN-HA間セキュリティは、独立である。このた

め、HAは、オリジナルパケット356にIPsec処理が施されている場合であってもオリジナルパケット356にIPsec用ヘッダ357を付加する場合がある。

- 上記パケットを受信したMNは、受信パケットに対して、同一レイヤのセキュリティ処理を2度行う必要がある。しかし、通常のMNは、受信パケットに対して2重にIPsecを終端する処理を持たないという課題がある。

ここで、OSI参照モデルを説明する。OSI (Open Systems Interconnection) では、ネットワークを階層化した参照モデルが規定されている。この参照モデルは、7つの階層で表現されている。各階層を「レイヤ」と呼ぶ。最下層はレイヤ1であり、最上層はレイヤ7である。各レイヤ間の通信手順は、プロトコルで定義される。IPプロトコルやIPsecは、レイヤ3のプロトコルである。

- さらに、ネットワーク単位でモビリティを管理するネットワークにおいて、移動ネットワークが入れ子になる場合、IPinIPカプセル化を最低2重に処理する通信装置が必要である。しかし、通常の通信装置は、受信パケットに対して、IPinIPカプセル化を複数回終端する処理を持たない。すなわち、多重IPinIPカプセル化は、通信装置が特殊なIP層処理機能を備えなければ処理できない。

本発明の目的は、Mobile IPv6 サービスを提供可能な端末を実現することにある。

特に、アプリケーションがIPv6に対応していない端末に対して、Mobile IPv6 サービスによる通信方法を提供することにある。

- 本発明のその他の目的は、移動端末に対して、移動端末が接続される網状態に応じて通信方法を切り替える通信方法を提供す

ることにある。

本発明のその他の目的は、移動端末に対して、セキュリティ管理形態に応じたセキュリティ機能を複数回処理する手段を提供することにある。

- 5 本発明のその他の目的は、カプセル化機能を複数回処理する手段を提供することにある。

(解決手段)

上記の問題を解決するために、本発明は、従来の端末装置に加えて少なくとも以下の手段を備える。すなわち、

- 10 (1) Mobile IPv6機能を備える端末装置がIPアドレス変換機能を備える。上記端末装置は、IPv6アドレス体系に従うパケットを受信したとき、Mobile IPv6処理を行った後IPアドレスを変換する手段と、IPパケットを送信するとき、IPアドレスの変換を行った後、Mobile IPv6処理を行う手段  
15 を備える。
- (2) あるいは、上記端末装置がIPsec処理機能またはIPカプセル化を備える場合、上記端末装置がパケットを受信したとき、Mobile IPv6処理を行った後Mobile IPに関するIPsec処理またはIPデカプセル化処理を行う手段と、上記端末装置がパケットを送信するとき、送信パケットに対して  
20 Mobile IPに関するIPsec処理またはIPカプセル化処理を行った後Mobile IPv6処理を行う手段を備えてもよい。
- (3) あるいは、上記端末装置がHMIPv6機能を備え、上記端末装置がパケットを受信したときHMIPv6処理を行った後  
25 Mobile IPv6処理を行う手段と、上記端末装置がパケットを送信するときMobile IPv6処理を行った後HMIPv6処理を

行う手段を備えてもよい。上記HMIPv6処理は、IPsec処理  
或いはIPカプセル化・デカプセル化処理を含む。

(4) さらに、上記端末装置がMobile IPの制御信号を検出し、  
上記(1)から(3)の通信方法を選択する手段を備えて  
5 もよい。

(5) あるいは、上記端末装置が、Mobile IPに関するセキュ  
リティ処理機能とは別に、セキュリティ処理手段を備えて  
もよい。

あるいは、Network Mobilityを備える通信網における通信装置が、  
10 上記(2)に記載の packets 処理手段を備えてもよい。

(発明の効果)

本発明は Mobile IPv6 サービスを提供可能な移動端末装置、移動  
端末制御方法を提供する。

特に、端末装置が IPv6 アドレス体系に従う packets を受信した  
15 とき、Mobile IPv6 処理を行った後 IP アドレスを変換する手段と  
、IP packets を送信するとき、IP アドレスの変換を行った後、  
Mobile IPv6 処理を行う手段を備えることにより、アプリケーション  
が IPv6 に対応していなくても、Mobile IPv6 サービスを利用でき  
る端末装置の実現が可能になる。

20 あるいは、端末装置が IPsec 処理機能または IP カプセル化・デカ  
プセル化処理機能を備える場合、上記端末装置が packets を受信  
したとき、Mobile IPv6 処理を行った後 IPsec 処理または IP デカプ  
セル化処理を行う手段と、上記端末装置が packets を送信する  
とき、送信 packets に対して IPsec 処理または IP カプセル化処理を  
25 行った後 Mobile IPv6 処理を行う手段を備えることにより、より  
複雑な処理を行う端末装置の実現が可能になる。

あるいは、上記端末装置がさらに HMIPv6 機能を備え、上記端末装置がパケットを受信したとき HMIPv6 処理を行った後 Mobile IPv6 処理を行う手段と、上記端末装置がパケットを送信するとき Mobile IPv6 処理を行った後 HMIPv6 処理を行う手段を備えること  
5 により、Mobile IPv6 対応かつ、HMIPv6 対応の端末装置の実現が可能になる。

さらに、上記端末装置が Mobile IP の制御信号を検出し、適切な通信方法を選択する手段を備えることにより、通信網に応じて通信方法を切り替える端末装置の実現が可能になる。

10 さらに、上記端末装置が、Mobile IP に関するセキュリティ処理機能とは別に、セキュリティ処理手段を備えることにより、端末装置が同一レイヤのセキュリティ処理を複数回終端することが可能になる。

さらに、Network Mobility 機能を備える通信網における HA が、パ  
15 ケットを受信したとき、Mobile IPv6 処理を行った後 IPsec 処理または IP デカプセル化処理を行う手段と、上記端末装置がパケットを送信するとき、送信パケットに対して IPsec 処理または IP カプセル化処理を行った後 Mobile IPv6 処理を行う手段を備えることにより、Network mobility を持った HA の実現が可能になる。

20

#### 図面の簡単な説明

図 1 は、本発明における通信網の構成例を示す構成図である。図 2 は、MN 1 のブロック図である。図 3 は、MN 1 が備える Binding Update List 管理テーブル図である。図 4 は、MN 1 が備えるシナ  
25 リオポリシー管理テーブル図である。図 5 は、MN 1 のブロック図その 2 である。図 6 は、MN 1 が備える IPv4-IPv6 変換テーブル図であ

る。図 7 は、IPv6 パケットのフォーマット図である。図 8 は、Binding Acknowledgement メッセージ例の図である。図 9 は、MN1 のシナリオ処理部が備える BA 処理ルーチン図である。図 10 は、第 1 の実施例における位置登録・パケット送受信シーケンス図である。図 11 は、カプセル化パケットのフォーマット図である。図 12 は、第 2 の実施例における位置登録・パケット送受信シーケンス図である。図 13 は、MN1 の Mobile IPv6 処理部が備える BA 処理ルーチン図である。図 14 は、Binding Acknowledgement メッセージ例の図その 2 である。図 15 は、MN1 のシナリオ処理部が備える BA 処理ルーチン図その 2 である。図 16 は、MN1 のシナリオ処理部が備える BA 処理ルーチン図その 3 である。図 17 は、MN1 の IPv6 パケット処理部が備えるパケット送信処理ルーチン図である。図 18 は、MN1 の IPv6 パケット処理部が備えるパケット受信処理ルーチン図である。図 19 は、第 3 の実施例における位置登録・パケット送受信シーケンス図その 1 である。図 20 は、第 3 の実施例における位置登録・パケット送受信シーケンス図その 2 である。図 21 は、第 3 の実施例における位置登録・パケット送受信シーケンス図その 3 である。図 22 は、第 3 の実施例における位置登録・パケット送受信シーケンス図その 4 である。図 23 は、第 5 の実施例における通信網の構成例を示す構成図である。図 24 は、第 5 の実施例における位置登録・パケット送受信シーケンス図その 1 である。図 25 は、第 5 の実施例における位置登録・パケット送受信シーケンス図その 2 である。図 26 は、第 5 の実施例における位置登録・パケット送受信シーケンス図その 3 である。図 27 は、第 6 の実施例における通信網の構成例を示す構成図である。図 28 は、第 6 の実施例における MN1 のプロ

ック図である。図 29 は、第 6 の実施例における Router Advertisement メッセージ例の図である。図 30 は、MN1 のシナリオ処理部が備える BA 処理ルーチン図その 4 である。図 31 は、第 6 の実施例における位置登録・パケット送受信シーケンス図その 1 である。図 32 は、第 6 の実施例における位置登録・パケット送受信シーケンス図その 2 である。図 33 は、第 6 の実施例における位置登録・パケット送受信シーケンス図その 3 である。図 34 は、第 7 の実施例における通信網の構成例を示す構成図である。図 35 は、第 7 の実施例における HA のブロック図である。図 36 は、モバイルトンネル適用区間を示す図である。図 37 は、セキュリティ適用区間を示す図である。図 38 は、第 8 の実施例における通信網の構成例を示す構成図である。図 39 は、第 8 の実施例における TLS を用いた通信シーケンス図である。

## 15 発明を実施するための最良の形態

### (実施例 1)

本発明の第 1 の実施の形態を図面を用いて説明する。

代表例として、Mobile IPv6 対応移動ノード (MN) がホームリンク (以下、ホーム網) 以外の網 (以下、在圏網) に移動した際の通信方法を詳細に説明する。

図 1 は、本発明における通信網の構成例を示す。本発明における通信網は MN1 のホーム網 6 と IP 網 7 と在圏網 5 (5a、5b) から構成される。本実施例において、ホーム網 6、IP 網 7、及び在圏網 5 は IPv6 網である。MN1 は Mobile IPv6 対応移動ノード (MN) である。在圏網 5 と IP 網 7、及び、IP 網 7 とホーム網 6 は、ルータ、或いは、ゲートウェイ装置を介して接続される。在圏網 5 とホーム網 6 は、

ルータ、或いは、ゲートウェイ装置を介して接続されてもよい。

ホーム網6は、HA4を備える。在圏網5 (5a、5b) は、IP網7とのインタフェースをもつルータ3 (3a、3b) を備える。

HA4はMobile IPv6対応ホームエージェント (HA) である。HA4  
5 はホーム網6以外に存在するMN1の位置情報を管理する。上記位置情報は、MNのホームアドレスと気付アドレスのバインディング情報である。HA4は通信相手端末 (CN) 2がMN1のホームアドレス宛に送信するパケットを捕捉して、在圏網5bに存在するMN1にパケットを転送する機能を備える。

10 図2はMN1のメモリなど記憶装置に格納されたプログラムによって実現されるアプリケーションの構成例を示す。MN1は、ホストOS13と、ホストOS上のアプリケーション空間11と、仮想マシン12とから構成される。

仮想マシン12は、ゲストOS17とゲストOS上のアプリケーション  
15 空間16とから構成される。

ゲストOS17はMobile IPv6処理部25と、ホストOS13とゲストOS17を接続する仮想通信網15と、ゲストOS17と外部通信網とを接続する仮想通信網14とを備える。Mobile IPv6処理部25は、Mobile IPv6のMN (Mobile Node) 機能を備え、Binding Update List管理  
20 テーブル210と、BA処理ルーチン70を含む。

アプリケーション空間16は、IPパケット処理部22とシナリオ処理部23とIPv6パケット処理部24とシナリオポリシ21とを備える。IPパケット処理部22は、ホストOS13とのパケット入出力機能を備える。IPv6パケット処理部24は、外部通信網とのパケット送受信  
25 機能を備える。シナリオポリシ21は、MN1の通信方法を管理する機能を備え、シナリオポリシ管理テーブル220を含む。

本実施例において、MN1は仮想マシンを搭載している。仮想マシンの代わりに、MN1が仮想マシンに相当するプログラムを搭載してもよい。

図3はBinding Update List管理テーブル210のテーブル構成の一例を示す。Binding Update List管理テーブル210は、Binding Update送信先アドレス211に対して、少なくともMNのホームアドレス212、MNが在圏網で取得したCare of Address (CoA) 213の対応関係を格納する。上記Binding Update List管理テーブル210は、Binding Cacheの有効期間を示すLifetime214を含んでもよい。

10 Binding Update List管理テーブル210がLifetime214を含む場合、MN1は上記テーブルは有効期限が切れたエントリを削除できる。

図4はシナリオポリシ管理テーブル220のテーブル構成の一例を示す。シナリオポリシ管理テーブル220はシナリオ番号221に対して、少なくともシナリオの処理内容を示すシナリオ内容222と、状態223との対応関係を格納する。

15

図5はMN1がIPアドレス変換機能を備える場合の構成例を示す。図5に示す各構成要素は、メモリなど記憶装置に格納されたプログラムによって実現される。シナリオ処理部23がIPv4-IPv6変換機能と、IPv4-IPv6変換テーブル230とを備える。パケット処理部

20 22は、IPv4パケット入出力機能を備える。

図6はIPv4-IPv6変換テーブル230のテーブル構成の一例を示す。IPv4-IPv6変換テーブル230はIPv6アドレス231に対して、少なくともIPv4アドレス232との対応関係を格納する。IPv4-IPv6変換テーブル230は、変換エントリの有効期限を示すLifetime233との対応関係を含んでもよい。IPv4-IPv6変換テーブル230がLifetime233を含む場合、MNは、有効期限がきれたエントリを削

25

除できる。

図10に示すシーケンスに従って、図1に示す網5bに在圏するMN1がHA4に位置登録を行い、パケットを送受信するシーケンスを説明する。

- 5      ここで、シナリオポリシ管理テーブル220は、「IPv4-IPv6変換機能有IPsecなし」が有効になっているものとする。このとき、IPv6パケット処理部24は、MN1が受信する全パケットの処理を行う。

- 10      MN1は在圏網5bに属するルータ3bからルータ広告（Router Advertisement）を受信して、CoAを取得する。MN1は、仮想通信網14へのインタフェース部18に気付アドレスを設定する。即ち、上記インタフェース部18と気付アドレスの対応情報をMN1のプログラムが保持する。

- 15      在圏網5bでCoAを取得したMN1は、HA4に位置登録メッセージ（Binding Update）を送信する（501）。

Binding Updateメッセージを受信したHA4は、MN1の位置登録情報を更新し、MN1のプロキシとして動作する。

HA4はMN1にBinding Updateの応答（Binding Acknowledgement）を送信する（502）。

- 20      図7は、IPv6パケットフォーマットを示す。IPv6パケットは、IPv6基本ヘッダ41と、拡張ヘッダ42と、ペイロード43とから構成される。基本ヘッダ41は、送信元アドレス41aと、着信先アドレス41bとを含む。

- 25      図8は、Binding Acknowledgementメッセージのフォーマット例S1を示す。IPv6 Routing Header421とIPv6 Mobility Header422は、IPv6パケットの拡張ヘッダ42に格納される。HA4がMN1に送信

- するBinding Acknowledgementは、以下の値が格納される。IPv6  
パケットヘッダの着信先アドレス41bに在圏網5bで取得した気付  
アドレスを格納する。着信先アドレス41bにMN1のホームアドレス  
以外の値を格納する場合、IPv6 Routing Header421のHome  
5 Addressフィールド4211にMN1のホームアドレスを格納する。

MN1のMobile IPv6処理部25は、Binding Updateが正常に終了し  
たことを示すBinding Acknowledgementを受信すると、HA4に対応  
するエントリをBinding Update List管理テーブルに登録する  
(503)。

- 10 IPv6パケット処理部24は、受信パケットがIPv6 Mobility  
Header422を含み、MHタイプ4221にBAを示すコードが含まれば、  
受信パケットがBinding Acknowledgementであると判断する。  
IPv6パケット処理部24は、Mobile IPv6のBinding  
Acknowledgementが入力されると(504)、入力パケットにシナリオ  
15 識別子を含むヘッダを付加する。シナリオ識別子には、  
「IPv4-IPv6変換有IPsecなし」を示す番号(10000)を設定する。  
IPv6パケット処理部24は、ヘッダ付きパケットをシナリオ処理部  
23に出力する。図11は、付加ヘッダ付パケットのフォーマット例  
S3を示す。入力パケットに対して、UDPヘッダ44を付加する。UDP  
20 ヘッダ44のDestination Portフィールド45にシナリオ識別子を  
設定する。

- シナリオ識別子を付加することにより、MNは、シナリオ処理部  
23が備える複数のプログラムから起動するプログラムを選択す  
ることが可能になる。また、シナリオ処理部23に対して機能の追  
25 加が行いやすくなるため、MN1の拡張性が増す。

シナリオ処理部23は、BA処理ルーチン60を起動して、付加ヘッ

ダの識別子からシナリオを決定し(61、505)、付加ヘッダを削除する。「IPv4-IPv6変換有IPsecなし」の場合、まず、Binding AcknowledgementメッセージのStatusフィールド4222を参照する(62)。Statusフィールドの値が128より小さければ、シナリオ処理部23は、HAアドレスと、気付アドレスを取得する。HAアドレスは、受信パケットの送信元アドレス41aから取得する。CoAは、受信パケットの着信先アドレス41bから取得する。次にIPv6パケット処理部24にIPinIPトンネル情報を設定する(63、506)。IPv6パケット処理部24は、IPinIPトンネル用のインタフェースを保持する。このIPinIPトンネル用のインタフェースに対して、少なくともトンネルの始点アドレスと終点アドレスを対応つける。

続いて、MN1のホームアドレスを取得する。MN1のホームアドレスは、Binding AcknowledgementメッセージのIPv6 Routing Header421内Home Address4211から取得する。ここで、シナリオ処理部23はMN1のホームアドレスでIPv4-IPv6変換テーブル230を検索する。該当エントリが存在すれば、該当エントリの有効期限を更新し(64、507)、本ルーチンを終了する。該当エントリが存在しなければ、シナリオ処理部23は、仮想IPv4アドレスプールからIPv4アドレスを1つ選び、この仮想IPv4アドレスとMN1のホームアドレスを対応付けた新規変換エントリをIPv4-IPv6変換テーブル230に追加する。続いて、上記変換エントリのIPv4フィールド232に設定した仮想IPv4アドレスをインタフェース部19に設定し(64、507)、本ルーチンを終了する。仮想IPv4アドレスプールは、IPアドレス変換用に確保するIPv4アドレス群である。IPv6アドレス宛のパケットをIPv4ネットワークで識別するため、IPv6アドレスに対して仮想IPv4アドレスを対応付ける。MN1のプログ

ラムは、上記インタフェース部19と仮想IPv4アドレスの対応情報を保持する。

- ステップ62において、Binding AcknowledgementメッセージのStatusフィールド4222の値が128以上であれば、受信パケットを
- 5 廃棄して本ルーチンを終了する(67)。ステップ63においてIPinIPトンネル設定ができない場合、或いは、ステップ64において変換エントリの更新ができない場合、受信パケットを廃棄して本ルーチンを終了する(67)。HAは、Binding Updateの処理結果をBinding AcknowledgementメッセージのStatusフィールドの値で示す。
- 10 Status フィールドの値が128より小さい場合、HAがBinding Updateを許容したことを示す。dStatusフィールドの値が128以上の場合、HAがBinding Updateを拒否したことを示す。

ここで、図10に戻りパケットの送受信シーケンスの説明を続ける。

- 15 CN2がMN1にパケットを送信する際、CN2はパケットをMN1のホームアドレス宛に送信する(508)。HA4は上記パケットを捕捉し、IPヘッダを付加する(509)。以下、この付加したIPヘッダを外側IPヘッダと呼ぶ。外側IPヘッダの着信先アドレスには、MN1が在圏網5bで取得したCoAを設定する。外側IPヘッダの送信元アドレスには、HA4のアドレスを設定する。
- 20

- MN1のIPv6パケット処理部24は、パケット509を受信すると外側IPヘッダの送信元アドレスを確認する。外側IPヘッダの送信元アドレスがHA4のアドレスであれば、IPv6パケット処理部24は外側IPヘッダを削除し(デカプセル化)(510)、パケットをシナリオ処理部23に出力する。
- 25

シナリオ処理部23は、受信パケットのIPヘッダをIPv6からIPv4

に変換する(511)。まず、着信先アドレスでIPv4-IPv6変換テーブル230を参照する。上記変換テーブル230に該当エントリが存在すれば、このエントリに設定されたIPv6アドレスとIPv4アドレスの対応を用いて、着信先アドレスをIPv4に変換する。次に受信パケットの送信元アドレスで上記変換テーブル230を参照する。上記変換テーブル230に該当エントリが存在すれば、このエントリに設定されたIPv6アドレスとIPv4アドレスの対応を用いて送信元アドレスをIPv4に変換する。該当エントリが存在しなければ、シナリオ処理部23は、仮想IPv4アドレスプールからIPv4アドレスを1つ選択し、この仮想IPv4アドレスと送信元アドレスを対応付けた新規エントリを上記変換テーブル230に追加する。

シナリオ処理部23は、IPv4ヘッダを含むパケットをIPv4パケット処理部22経由でホストOS上のアプリケーション11に出力する(512)。

次にホストOS上のアプリケーション11がCN2にパケットを送信する方法を説明する。ホストOS上のアプリケーション11は、IPv4ヘッダを含むパケットを出力する(513)。IPv4パケット処理部22が上記パケットを入力し、シナリオ処理部23に出力する。まず、送信元アドレスでIPv4-IPv6変換テーブル230を参照する。上記変換テーブル230に該当エントリが存在すれば、送信元アドレスをIPv6に変換する。次にシナリオ処理部23は、パケットの着信先アドレスでIPv4-IPv6変換エントリ230を参照する。上記変換テーブル230に該当エントリが存在すれば、着信先アドレスをIPv6に変換する。該当エントリが存在しなければ、シナリオ処理部23は、仮想IPv6アドレスプールからIPv6アドレスを1つ選択し、この仮想IPv6アドレスと着信先アドレスを対応付けた新規エントリ

を上記変換テーブル230に追加する。

IPヘッダ変換後(514)、シナリオ処理部23はIPv6パケット処理部24にパケットを出力する。IPv6パケット処理部24は、ステップ506で設定したIPinIPトンネル情報を参照してIPヘッダを追加した後(カプセル化)(515)、パケットを送信する(516)。HA4は上記カプセル化ヘッダを削除した後、パケットをCN2に転送する(517)。

本発明の第1の実施の形態によると、端末装置のホストOSがMobile IPv6対応MN機能を備えない場合であっても、端末装置にMobile IPv6サービスの提供が可能になる。また、上記端末装置がIPアドレス変換機能を備えることにより、アプリケーションがIPv6に対応していない端末に対して、Mobile IPv6サービスの提供が可能になる。

#### (実施例2)

本発明の第2の実施の形態を図面を用いて説明する。第2の実施例は、第1の実施例において、IPv6対応アプリケーションを利用する端末装置にMobile IPv6サービスを提供する手段を備えることを特徴とする。

ここで、シナリオポリシー管理テーブル220は、「IPv4-IPv6変換機能なしIPsecなし」が有効になっているとする。このとき、IPv6パケット処理部24は、MNが受信する全パケットを処理する。

図12に示すシーケンスに従って、図1に示す網5bに在圏するMN1がHA4に位置登録を行い、パケットを送受信するシーケンスを説明する。

MN1が在圏網でCoAを取得し、位置登録を行うまでの処理(ステップ501からステップ504)は、第1の実施例と同じである。

IPv6 パケット処理部 24 は、 Mobile IPv6 の Binding Acknowledgement 信号を入力すると (504)、受信パケットにシナリオ識別子を含むヘッダを付加する。シナリオ識別子には、「IPv4-IPv6 変換なし IPsec なし」を示す番号 (10001) を設定する。IPv6 パケット処理部 24 は、ヘッダ付きパケットをシナリオ処理部 23 に出力する。

シナリオ処理部 23 は、BA 処理ルーチン 60 を起動して、付加ヘッダの識別子からシナリオを決定し (61、505)、付加ヘッダを削除する。「IPv4-IPv6 変換なし IPsec なし」である場合、第 1 の実施例におけるステップ 62 とステップ 63 と同様に、Binding Acknowledgment メッセージの Status フィールド 4222 のチェック (65) と IPinIP トンネル設定処理 (66、506) を行い、本ルーチンを終了する。IPinIP トンネル設定処理 (66、506) の処理は、実施例 1 と同様である。

なお、ホスト OS のインタフェース部 19 には、MN 1 のホームアドレスを設定する。即ち、MN 1 のプログラムは、上記インタフェース部 19 に MN 1 のホームアドレスを対応付ける。

次にパケットの受信方法を説明する。ステップ 508 からステップ 510 は、第 1 の実施例と同様である。IPv6 パケット処理部 24 は、デカプセル化処理終了後のパケットに IP アドレス変換を行うことなく、IP パケット処理部 22 経由でホスト OS に対して出力する (512)。

次にパケットの送信方法を説明する。シナリオ処理部 23 がホスト OS のアプリケーション 11 からパケットを入力すると (513)、IP アドレス変換を行うことなく、IPv6 パケット処理部 24 に出力する。ステップ 515 からステップ 517 は、第 1 の実施例と同様である。

本発明の第2の実施の形態によると、端末装置のホストOSが Mobile IPv6対応MN機能を備えない場合であっても、端末装置に Mobile IPv6サービスの提供が可能になる。また、端末装置のホストOSのインタフェース部にMNのホームアドレスの設定が可能  
5 になる。

(実施例3)

本発明の第3の実施の形態を図面を用いて説明する。

第3の実施例は、第1の実施例に加えて、Mobile IP信号に IPsecを適用する端末装置に Mobile IPv6サービスを提供する手  
10 段を備えることを特徴とする。

IPsecは、IETFが標準化を行うセキュリティ機能である。IPsecは、パケットの認証機能と暗号化機能を備える。IPsecによる認証機能が適用されたIPパケットは、認証ヘッダ（AH: Authentication Header）を含む。IPsecによる暗号化機能が適用  
15 されたIPパケットは、暗号化ペイロード（ESP: Encapsulating Security Payload）ヘッダを含む。

図19から図22に示すシーケンスに従って、図1に示す網5bに在圏するMN1がHA4に位置登録を行い、パケットを送受信するシーケンスを説明する。

20 ここで、シナリオポリシ管理テーブル220は、「IPv4-IPv6変換機能有」又は、「IPv4-IPv6変換有経路最適化有」が有効になっているものとする。このとき、IPv6パケット処理部24は、MNが受信する全パケットを処理する。

第3の実施例において、Mobile IPv6処理部25はBA処理ルーチン70を備える。第3の実施例において、IPv6パケット処理部24  
25 はパケット送信処理ルーチン100と、パケット受信処理ルーチン

120と、Binding Update List管理テーブル210を備える。

まず、図19を用いて、HA4に位置登録を行ったMN1の packets 送受信シーケンスを説明する。

- MN 1 が 在 圏 網 で CoA を 取 得 し 、 HA4 から Binding Acknowledgementメッセージを受信するまでの処理(ステップ501、ステップ502)は、第1の実施例と同じである。第3の実施例において、Binding Acknowledgementメッセージには、IPsecが施されている。すなわち、Binding Acknowledgementメッセージを含むIP packets は、少なくともESPヘッダを含む。上記 packets が、
- 10 AHヘッダを含んでもよい。

図14にIPsec付Binding Acknowledgementメッセージのフォーマット例S2を示す。IPsec (AHヘッダ又はESPヘッダ) 423は、IPv6 Routing Header421とIPv6 Mobility Header 422の間に設定される。

- 15 Mobile IPv6 処理部 25 は、 Mobile IPv6 の Binding Acknowledgementメッセージを受信すると、BA処理ルーチン70を起動する。まずIPv6 Routing Header 421の処理を行い(71)、Routing Headerに設定されたMN1のホームアドレス4211とIPv6着信先アドレス41bに設定されたMN1のCoAを入れ替える。次にIPv6
- 20 ヘッダ41のNext Header値が、IPsecであるか確認する(72)。Next HeaderがIPsecであれば、IPsecヘッダのSAを決定し、受信 packets に対してIPsec処理(認証処理、暗号復号化処理)を行う(73)。
- 続いて、SPDを参照して、セキュリティポリシーに合致することを確認する(74)。その後、Mobile IPv6 処理部は、Binding Acknowledgementメッセージを処理する。Mobile IPv6処理部は、Binding Acknowledgementメッセージの送信元アドレスで

Binding Update List管理テーブル210を検索する。該当エントリがあれば、エントリの更新を行う。該当エントリがなければ、新規エントリを追加する(75、503)。

続いて、Mobile IPv6処理部25は、受信パケットにシナリオ識別子を含むヘッダを付加したパケットをシナリオ処理部23に送信し(76、521、522)、本ルーチンを終了する。Binding Acknowledgement送信元がHAである場合、シナリオ識別子にはIPv4-IPv6変換を示す番号(10010)を設定する。

ステップ72でNext HeaderがIPsecではない場合、ステップ74に進む。

ステップ73でMobile IPv6処理部25がSAを決定できなかった場合、或いは、ステップ74で受信パケットがセキュリティポリシーを満たさなかった場合、或いは、ステップ75でBinding Update List管理テーブル210を更新できなかった場合、受信パケットを廃棄し(77)、本ルーチンを終了する。

シナリオ処理部23は、BA処理ルーチン60を起動して、付加ヘッダの識別子からシナリオを決定し(61、505)、付加ヘッダを削除する。IPv4-IPv6変換有の場合、シナリオ処理部23はHAアドレスと気付アドレスを取得し、IPv6パケット処理部24にIPinIPトンネル情報を設定する(81、506)。次にMN1のホームアドレスを取得し、変換エントリの生成・更新を行い、本ルーチンを終了する(82、507)。ステップ81とステップ82の処理は、第1の実施例のステップ63、ステップ64の処理と同様である。

ステップ81でIPinIPトンネル情報が設定できなかった場合、ステップ82で変換エントリの生成・更新ができなかった場合は、受信パケットを廃棄し(67)、本ルーチンを終了する。

ここで、図19に戻りパケットの送受信シーケンスの説明を続ける。

- CN2がMN1にパケットを送信する際、CN2はMN1のホームアドレス宛にパケットを送信する(508)。HA4は上記パケットを捕捉し、
- 5 IPヘッダを付加する(509)。外側IPヘッダの着信先アドレスには、MN1が在圏網5bで取得したCoAが設定される。外側IPヘッダの送信元アドレスには、HA4のアドレスが設定される。

MN1のIPv6パケット処理部24は、パケット509を受信するとパケット受信処理ルーチン120を起動する。

- 10 IPv6パケット処理部は、パケット509を受信するとMN1がホーム網に存在するか否かを判断する(121)。ステップ506においてCoAを取得済みであるため、IPv6パケット処理部24は、MN1がホーム網以外に存在すると判断する。続いて、受信パケットのNext Header値を参照する。Next Header値がIPヘッダであれば、外側
- 15 IPヘッダの送信元アドレスを確認する。外側IPヘッダの送信元アドレスがHA4のアドレスであれば、IPv6パケット処理部24は外側IPヘッダを削除する(デカプセル化)(128、510)。次にセキュリティポリシーの有無を確認する(129)。セキュリティポリシーが存在しなければ、パケットをシナリオ処理部23に送信し(127)、本
- 20 ルーチンを終了する。

- ステップ129において、セキュリティポリシーが存在する場合、受信パケットが上記ポリシーを満たすか否かを確認する(126)。セキュリティポリシーを満たす場合は、パケットのNext Header値を参照する。Next Header値がIPヘッダでなければ(131)、受信パ
- 25 ケットをシナリオ処理部23に送信し(127)、本ルーチンを終了する。

ステップ126において、セキュリティポリシーを満たさない場合は受信パケットを廃棄し（130）、本ルーチンを終了する。

ステップ128において、外側IPヘッダの送信元アドレスがHA4のアドレスでなければ、受信パケットを廃棄し（130）、本ルーチンを終了する。

ステップ511、512は、第1の実施例と同様である。

次にホストOS上のアプリケーション11がCN2にパケットを送信する方法を説明する。ステップ513、514は、第1の実施例と同様である。

10 IPヘッダ変換後（514）、シナリオ処理部23はIPv6パケット処理部24にパケットを送信する。IPv6パケット処理部24は、パケット送信処理ルーチン100を起動する。

IPv6パケット処理部は、パケット514を受信するとMN1がホーム網に存在するか否かを判断する（101）。ステップ506においてCoA  
15 を取得済みであるため、IPv6パケット処理部24は、MN1がホーム網以外に存在すると判断する。続いて着信先アドレス41bで、Binding Update List管理テーブル210を参照する（102）。上記Binding Update List管理テーブル210に該当エントリが存在しなければ、セキュリティポリシーの有無を確認する（108）。セキュリティ  
20 ポリシーが存在しなければ、IPv6パケット処理部は、ステップ506で設定したIPinIPトンネル情報を参照してIPヘッダを追加する（カプセル化）（515、111）。そして、パケットを送信し（107）、本ルーチンを終了する。

ステップ516、517は、第1の実施例と同様である。

25 ステップ109において、パケットを廃棄すべきと判断した場合、或いは、ステップ110において、SAが検出できなかった場合、

受信パケットを廃棄して(112)、本ルーチンを終了する。

図20は、MN1がCN2との間でMobile IPv6の経路最適化処理を行った場合のパケット送受信シーケンスを示す。

MN1のMobile IPv6処理部25は、MN1のCoAを通知するため、CN2  
5 にBinding Updateメッセージを送信する(531)。MN1のMobile IPv6処理部25はCN2からBinding Acknowledgementメッセージを受信する(532)。上記Binding Acknowledgementメッセージ532はIPsecを含まない。

Mobile IPv6処理部25は、Mobile IPv6のBinding  
10 Acknowledgementメッセージを受信すると、BA処理ルーチン70を起動する。まずRouting Header 421の処理を行う(71)。IPv6 Routing Headerに設定されたMN1のホームアドレス4211とIPv6着信先アドレス41bに設定されたMN1のCoAを入れ替える。次にIPv6ヘッダ41のNext Header値が、IPsecであるか確認する(72)。Next  
15 HeaderがIPsecではなければ、SPDを参照して、セキュリティポリシーに合致することを確認する(74)。その後、Mobile IPv6処理部25は、Binding Acknowledgementメッセージ処理を行う。Mobile IPv6処理部25は、Binding Acknowledgementメッセージの送信元アドレスでBinding Update List管理テーブル210を検索する。該  
20 当エントリがあれば、エントリの更新を行う。該当エントリがなければ、新規エントリを追加する(75、533)。

続いて、Mobile IPv6処理部25は、受信パケットにシナリオ識別子を含むヘッダを付加し、シナリオ処理部23に送信後(76、534、535)、本ルーチンを終了する。Binding Acknowledgementメッセージ532の送信元アドレスは、CNアドレスであり、HAアドレスではない。そこで、シナリオ識別子にはIPv4-IPv6変換有り経路最

適化有りを示す番号（10011）を設定する。

シナリオ処理部23は、BA処理ルーチン60を起動して、付加ヘッダの識別子からシナリオを決定し（61、536）、付加ヘッダを削除する。IPv4-IPv6変換有経路最適化有りの場合、まず、シナリオ

5 処理部23は、Binding Acknowledgementメッセージ532のMHタイプ4221を参照する（83）。MHタイプがBinding Acknowledgementメッセージを示す値であれば、IPv6パケット処理部24のBinding Update List管理テーブル210をBinding Acknowledgementメッセージの送信元アドレスで検索する。該当エントリがあれば、エン

10 トリの情報を更新する。該当エントリがなければ、新規エントリを上記テーブル210に追加する（84）。次にMN1のホームアドレスを取得し、変換エントリの生成・更新を行い、本ルーチンを終了する（82、537）。

ステップ84において、Binding Update List管理テーブル210

15 のエントリ更新或いはエントリ追加ができなかった場合、受信パケットを廃棄し（67）、本ルーチンを終了する。

ステップ83において、MHタイプがBinding Errorメッセージを示す値であれば、Binding Update List管理テーブル210から該当エントリを削除し（85）、本ルーチンを終了する。

20 ここで、図20に戻りパケットの送受信シーケンスの説明を続ける。

CN2がMN1にパケットを送信する際、MN1のホームアドレスでCN2のBinding Cache管理テーブルを参照する。CN2はステップ531でMN1のバインディング情報を取得している。従ってCN2は着信

25 先アドレス41bにMN1のCoAを、IPv6 Routing Header421にMN1のホームアドレスを、送信元アドレス41aにCN2のアドレスを、それぞ

れ設定したパケットを送信する(538)。

MN1のIPv6パケット処理部24は、パケット538を受信するとパケット受信処理ルーチン120を起動する。

- IPv6パケット処理部は、MN1がホーム網に存在するか否かを判断する(121)。ステップ506においてCoAを取得済みであるため、IPv6パケット処理部24は、MN1がホーム網以外に存在すると判断する。続いて、受信パケットのNext Header値を参照する。Next Header値がRouting Headerであれば、Routing Header処理を行う(123、539)。次にRouting HeaderのNext Header値を確認する(124)。
- 10 Next Header値がIPsecであれば、SAを検索しIPsec処理を行う(125)。次にセキュリティポリシーを確認する(126)。ステップ124において、Next Header値がIPsecでなければ、セキュリティポリシーの有無を確認する(129)。セキュリティポリシーが存在しなければ、パケットをシナリオ処理部23に送信し(127)、本ルーチンを
- 15 終了する。

- ステップ129において、セキュリティポリシーが存在する場合、受信パケットが上記ポリシーを満たすか否かを確認する(126)。セキュリティポリシーを満たす場合は、パケットのNext Header値を参照する。Next Header値がIPヘッダ
- 20 でなければ(131)、受信パケットをシナリオ処理部23に送信し(127)、本ルーチンを終了する。

ステップ126において、セキュリティポリシーを満たさない場合は受信パケットを廃棄し(130)、本ルーチンを終了する。

- ステップ125において、IPsec処理が正常に終了しなければ、受信パケットを廃棄し(130)、本ルーチンを終了する。
- 25

ステップ123において、Routing HeaderのHome Addressフイー

ルドにMN1のホームアドレスが設定されていなければ、受信パケットを廃棄し（130）、本ルーチンを終了する。

ステップ540、541は、第1の実施例のステップ511、512と同様である。

- 5 次にホストOS上のアプリケーション11がCN2にパケットを送信する方法を説明する。ステップ542、543は、第1の実施例のステップ513、ステップ514と同様である。

IPヘッダ変換後（543）、シナリオ処理部23はIPv6パケット処理部24にパケットを送信する。IPv6パケット処理部24は、パケット  
10 送信処理ルーチン100を起動する。

- IPv6パケット処理部は、MN1がホーム網に存在するか否かを判断する（101）。ステップ506においてCoAを取得済みであるため、IPv6パケット処理部24は、MN1がホーム網以外に存在すると判断する。続いて着信先アドレス41bで、Binding Update List管理テーブル210を参照する（102）。上記Binding Update List管理  
15 テーブル210には、ステップ537で生成したエントリが存在する。そこで、IPv6パケット処理部は、Destination Options HeaderのHome Address Optionを生成する（103、544）。Home Address Optionには、MN1のホームアドレスを設定する。送信元アドレス41aには、  
20 MN1のCoAを設定する。着信先アドレス41bには、CN2のアドレスを設定する。

次に、セキュリティポリシーの有無を確認する（104）。セキュリティポリシーが存在しなければ、IPv6パケット処理部は、パケットを送信し（107、545）、本ルーチンを終了する。

- 25 ステップ104において、セキュリティポリシーが存在する場合、送信パケットのセキュリティポリシーを決定する（105）。IPsec適用

時、IPv6パケット処理部は、SAを検索してIPsec処理を行う(106)。次に、パケットを送信し(107)、本ルーチンを終了する。IPsec非適用時、IPv6パケット処理部は、パケットを送信し(107)、本ルーチンを終了する。

- 5      ステップ105において、パケットを廃棄すべきと判断した場合、或いは、ステップ106において、SAが検出できなかった場合、IPv6パケット処理部は、受信パケットを廃棄して(112)、本ルーチンを参照する。

- 10      次に、図21を用いて、HA4に位置登録を行ったMN1がIPsec付モバイルIPトンネルを介してパケットを送受信する場合のシーケンスを説明する。

ステップ501から507までの処理は、図19と同様である。

- 15      CN2がMN1にパケットを送信する際、CN2はパケットをMN1のホームアドレス宛に送信する(508)。HA4は上記パケットを捕捉し、モバイルトンネルヘッダとIPsec機能付きIPヘッダ(IPsecトンネルモード)を付加する(551)。モバイルトンネルヘッダとIPsec機能付きIPヘッダの着信先アドレスには、MN1が在圏網5bで取得したCoAが設定される。モバイルトンネルヘッダとIPsec機能付きIPヘッダの送信元アドレスには、HA4のアドレスが設定される。

- 20      MN1のIPv6パケット処理部24は、パケット551を受信するとパケット受信処理ルーチン120を起動する。

- 25      IPv6パケット処理部は、パケット551を受信するとMN1がホーム網に存在するか否かを判断する(121)。ステップ506においてCoAを取得済みであるため、IPv6パケット処理部24は、MN1がホーム網以外に存在すると判断する。続いて、受信パケットのNext Header値を参照する。Next Header値がIPsecであれば、SAを検索

して、IPsec処理を行い、外側のIPヘッダを削除する（デカプセル化）（IPsec トンネルモード処理）（125、552）。次に受信パケットがセキュリティポリシーを満たすか否かを確認する（126、553）。セキュリティポリシーを満たす場合は、IPsec処理後のパケットの

5   Next Header値を参照する。

Next Header値がIPヘッダであれば、ステップ128を起動する。まず、外側IPヘッダの送信元アドレスを確認する。外側IPヘッダの送信元アドレスがHA4のアドレスであれば、IPv6パケット処理部24は外側IPヘッダを削除する（デカプセル化、510）。次に、

10   セキュリティポリシーの有無を確認する（129）。セキュリティポリシーが存在しなければ、パケットをシナリオ処理部23に送信し（127）、本ルーチンを終了する。

Next Header値がIPヘッダでなければ、パケットをシナリオ処理部23に送信し（127）、本ルーチンを終了する。

15   ステップ126において、セキュリティポリシーを満たさない場合は受信パケットを廃棄し（130）、本ルーチンを終了する。

ステップ125において、SAが検出できなければ、受信パケットを廃棄し（130）、本ルーチンを終了する。

ステップ511、512は、第1の実施例と同様である。

20   次にホストOS上のアプリケーション11がCN2にパケットを送信する方法を説明する。ステップ513、514は、第1の実施例と同様である。

IPヘッダ変換後（514）、シナリオ処理部23はIPv6パケット処理部24にパケットを送信する。IPv6パケット処理部24は、パケット

25   送信処理ルーチン100を起動する。

IPv6パケット処理部は、パケット514を受信するとMN1がホーム

- 網に存在するか否かを判断する(101)。ステップ506においてCoAを取得済みであるため、IPv6パケット処理部24は、MN1がホーム網以外に存在すると判断する。続いて着信先アドレス41bで、Binding Update List管理テーブル210を参照する(102)。上記
- 5 Binding Update List管理テーブル210に該当エントリが存在しなければ、セキュリティポリシーの有無を確認する(108)。

- セキュリティポリシーが存在する場合、送信パケットのセキュリティポリシーを決定する(109、554)。IPsec適用時は、SAを検索してIPsec処理(IPsec トンネルモード処理)とモバイルIPのカプセル化処理を行う(110、555)。その後、IPv6パケット処理部24
- 10 は、パケットを送信し(107、556)、本ルーチンを終了する。

次に、図22を用いて、HA4に位置登録を行ったMN1がIPsec付モバイルIPトンネルを介してパケットを送受信する場合の第2のシーケンスを説明する。

- 15 図21と図22は、HAとMNの間のパケットフォーマットが異なる。

図22におけるHA4は、モバイルトンネルヘッダとIPsec機能付きIPヘッダ(IPsecトンネルモード)の送信元アドレスと着信先アドレスがそれぞれ等しい場合、MN宛のパケットを捕捉し、IPsec機能付きIPヘッダ(IPsecトンネルモード)のみを付加する(557)。

- 20 IPsec機能付きIPヘッダの着信先アドレスには、MN1が在圏網5bで取得したCoAが設定される。IPsec機能付きIPヘッダの送信元アドレスには、HA4のアドレスが設定される。

MN1のIPv6パケット処理部24は、パケット557を受信するとパケット受信処理ルーチン120を起動する。

- 25 ステップ552、553(121、122、125、126)は、図21の場合と同様である。

ステップ131において、Next Header値はIPヘッダではないため、IPv6パケット処理部は、パケットをシナリオ処理部23に送信し(127)、本ルーチンを終了する。

ステップ511、512は、第1の実施例と同様である。

- 5 次にホストOS上のアプリケーション11がCN2にパケットを送信する方法を説明する。ステップ513、514は、第1の実施例と同様である。

IPヘッダ変換後(514)、シナリオ処理部23はIPv6パケット処理部24にパケットを送信する。IPv6パケット処理部24は、パケット  
10 送信処理ルーチン100を起動する。

ステップ554、555(101、102、108、109)は、図21の場合と同様である。

- ステップ110において、IPsec トンネルモード用のIPヘッダとモバイルトンネルヘッダの送信元アドレスと着信先アドレスが、  
15 それぞれ等しい場合、MNは SAを検索してIPsec用のヘッダ処理(IPsec トンネルモード処理)のみを行う(110、555)。その後、IPv6パケット処理部24は、パケットを送信し(107、558)、本ルーチンを終了する。

- 本発明の第3の実施の形態によると、端末装置のホストOSが  
20 Mobile IPv6対応MN機能を備えない場合であっても、Mobile IPv6処理をMobile IPv6処理部で行った後、ゲストOSのシナリオを起動することによって、端末装置に対してMobile IPv6信号にIPsecを適用したMobile IPv6サービスの提供が可能になる。

- また、ゲストOSのIPv6パケット処理部がBinding Update List  
25 を備えることにより、端末装置に対してモバイルIPv6の経路最適化サービスの提供が可能になる。

また、端末装置とHAとの間のモバイルトンネルにIPsecの適用が可能になり、安全性の高いサービスが提供できる。

- さらに、モバイルトンネル用のヘッダの送信元アドレスと着信先アドレスがIPsec用の送信元アドレスと着信先アドレスとそれぞれ等しい場合、モバイルトンネル用のヘッダを省略することが可能になり、サービスをより効率的に提供できる。

(実施例 4)

- 本発明の第 4 の実施の形態を図を用いて説明する。第 4 の実施例は、第 3 の実施例において、IPv6対応アプリケーションを利用する端末装置にMobile IPv6サービスを提供する手段を備えることを特徴とする。

第 4 の実施例において、シナリオポリシー管理テーブル220は、IPv4-IPv6変換機能なし又は、IPv4-IPv6変換なし経路最適化有りが有効になっているとする。

- 第 4 の実施例において、シナリオ処理部23は、図16に示すBA処理ルーチンを起動する。図16に示すBA処理ルーチンは、図15と比べて変換エントリ更新ステップを含まない点異なる。ステップ91からステップ94は、第 3 の実施例のステップ81、ステップ83からステップ85と同様である。

- 本発明の第 4 の実施の形態によると、IPv6対応アプリケーションを利用する端末装置のホストOSがMobile IPv6対応MN機能を備えない場合であっても、Mobile IPv6処理をMobile IPv6処理部で行った後、ゲストOSのシナリオを起動することによって、端末装置に対してMobile IPv6信号にIPsecを適用したMobile IPv6サービスの提供が可能になる。

また、ゲストOSのIPv6パケット処理部がBinding Update List

を備えることにより、モバイルIPv6の経路最適化サービスの提供が可能になる。

また、端末装置とHAとの間のモバイルトンネルにIPsecの適用が可能になり、安全性の高いサービスが提供できる。

- 5 さらに、モバイルトンネル用のヘッダの送信元アドレスと着信先アドレスがIPsec用の送信元アドレスと着信先アドレスとそれぞれ等しい場合、モバイルトンネル用のヘッダを省略することが可能になり、サービスをより効率的に提供できる。

(実施例 5)

- 10 本発明の第5の実施の形態を図を用いて説明する。第5の実施例は、第4の実施例において、端末装置がIPv6対応SIPによるVoIPサービスを利用する手段を備えることを特徴とする。第5の実施例において、シナリオポリシ管理テーブル220は、IPv4-IPv6変換機能なし又は、IPv4-IPv6変換なし経路最適化有りが有効になっ  
15 ているとする。

図23は、本発明における第5の実施例の通信網の構成例を示す。SIP Proxy8はルータに接続される。

図24、図25、図26は、第5の実施例におけるMN1の通信シーケンスである。

- 20 図24は、IPsecが端末間音声パケットに適用される場合のMN1の通信シーケンスを示す。

ステップ501からステップ506は、図19と同様であるため、ステップ561以降の処理を説明する。

- 25 CN2は、SIP Proxy8経由で、MN1にSIP INVITEメッセージを送信する(561、562)。MN1のホストOS上のアプリケーションが、上記メッセージを受信する。上記メッセージを受け付ける場合、

MN1のホストOS上アプリケーションは、上記INVITEに対する応答メッセージ（200 OK）を送信する。この応答メッセージは、SIP Proxy8経由でCN2へ送信される（563、564）。この応答メッセージは、MN1が音声パケットを受信するIPアドレスの情報として、MN  
5 1のホームアドレスを含む。

CN2は、上記応答メッセージを受信し、応答確認メッセージ（ACK）をMN1へ送信する（565、566）。以上で、CN2とMN1の間にセッションが確立する。

なお、SIP Proxy8がMN1のバインディング情報を保持しない場合、MN1とSIP Proxy8の間で送受信されるメッセージは、HA4を  
10 経由する。

続いて、CN2は、MN1のホームアドレス宛に音声パケット（RTPパケット）を送信する（567）。トランスポートモードのIPsecが、上記音声パケットに適用されている。

15 HA4は、上記パケットを捕捉して、カプセル化を行いMN1のCoA宛に送信する（568）。

IPv6パケット処理部24は、上記パケットを受信する。ステップ510は、図19と同様である。

IPv6パケット処理部24は、受信パケットをIPパケット処理部  
20 22経由でホストOSに送信する（570）。ステップ570は、ステップ512と比べて、オリジナルパケットに対してIPsecが施されている点異なる。ホストOSは、オリジナルパケットのIPsec処理を行った後、音声パケットの処理を行う。

次に、MN1がCN2に音声パケットを送信する手順を述べる。MN1  
25 は音声情報を含むIPパケットにIPsec処理を行い、パケットを送信する（571）。IPv6パケット処理部24は、パケットにモバイルト

ンネル用のヘッダを付加（カプセル化）する（515）。その後、IPv6パケット処理部は、パケットをHA4経由（574）でCN2宛に送信する（575）。

図25は、IPsecが端末間音声パケットとモバイルトンネルに適用される場合のMN1の通信シーケンスを示す。

HA4とMN1のモバイルトンネルには、トンネルモードIPsecが適用されとする。

ステップ561からステップ566は、図24と同じであるため、ステップ567以降の処理を説明する。

10 CN2が音声パケットをMN1のホームアドレス宛に送信する（567）。HA4は上記パケットを捕捉し、モバイルトンネルヘッダとIPsec機能付きIPヘッダ（IPsec トンネルモード）を付加する（581）。モバイルトンネルヘッダとIPsec機能付きIPヘッダの着信先アドレスには、MN1が在圏網5bで取得したCoAが設定される。モバイル  
15 トンネルヘッダとIPsec機能付きIPヘッダの送信元アドレスには、HA4のアドレスが設定される。

IPv6パケット処理部24は、上記パケットを受信すると、SA処理およびデカプセル化処理（IPsecトンネルモード処理）（568）、SPD検査処理（569）、デカプセル化（510）を行う。

20 ステップ568、569、510の処理は、図21のステップ552、553、510の処理と同じであるため、詳細は省略する。IPv6パケット処理部24は、IPパケット処理部22経由でホストOSにパケットを送信する（570）。ホストOSはIPsec付パケット570を受信すると、IPsec処理を行った後、音声パケットの処理を行う。

25 次に、MN1がCN2に音声パケットを送信する手順を述べる。MN1は音声情報を含むIPパケットにIPsec処理を行い、パケットを送

信する(571)。IPv6パケット処理部24は、SPD検査処理(572)、IPsec処理(IPsec トンネルモード処理)とモバイルIPのカプセル化処理(573)を行う。ステップ572、573は、図21のステップ554、555の処理と同じであるため、詳細は省略する。続いて、IPv6パケット処理部24が、パケットをHA4経由(582)でCN2宛に送信する(575)。

図26は、IPsecが端末間音声パケットとモバイルトンネルに適用される場合のMN1の通信シーケンスを示す。

ステップ561からステップ566は、図24と同じであるため、ステップ567以降の処理を説明する。

図25と図26は、HAとMNの間のパケットフォーマットが異なる。CN2が音声パケットをMN1のホームアドレス宛に送信する(567)。図26におけるHA4は、MN宛のパケット(567)を捕捉し、IPヘッダ(IPsec トンネルモード)のみを付加する(583)。外側IPヘッダの着信先アドレスには、MN1が在圏網5bで取得したCoAが設定される。外側IPヘッダの送信元アドレスには、HA4のアドレスが設定される。

IPv6パケット処理部24は、上記パケットを受信すると、SA処理およびデカプセル化処理(IPsecトンネルモード処理)(568)、SPD検査処理(569)を行う。

ステップ568、569の処理は、図22のステップ552、553の処理と同じであるため、詳細は省略する。IPv6パケット処理部24は、IPパケット処理部22経由でホストOSにパケットを送信する(570)。ホストOSはIPsec付パケット570を受信すると、IPsec処理を行った後、音声パケットの処理を行う。

次に、MN1がCN2に音声パケットを送信する手順を述べる。MN1

は音声情報を含むIPパケットにIPsec処理を行い、パケットを送信する(571)。IPv6パケット処理部24は、SPD検査処理(572)、IPsec処理(IPsec トンネルモード処理)(573)を行う。ステップ572、573は、図22のステップ554、555の処理と同じであるため、  
5 詳細は省略する。続いて、IPv6パケット処理部24が、パケットをHA4経由(584)でCN2宛に送信する(575)。

本発明の第5の実施の形態によると、IPsec付IPv6対応アプリケーションを利用する端末装置のホストOSがMobile IPv6対応MN機能を備えない場合であっても、Mobile IPv6処理をMobile IPv6  
10 処理部で行った後、ゲストOSのシナリオを起動することによって、端末装置に対してMobile IPv6信号にIPsecを適用したMobile IPv6サービスの提供が可能になる。

また、Mobile IPのIPsec処理部とアプリケーションのIPsec処理部を分離することにより、端末装置とHAとの間のモバイルトンネルにIPsecを適用する場合であっても、IPsec付アプリケーション  
15 の利用が可能になる。

#### (実施例6)

本発明の第6の実施の形態を図を用いて説明する。第6の実施例は、端末装置がMobile IPv6機能と、HMIPv6機能を備えることを特徴とする。第6の実施例において、シナリオポリシ管理テーブル220はMAPタイプ1から3が有効になっているものとする。  
20

図27は、本発明における第6の実施例の通信網の構成例を示す。ルータ3がHMIPv6のMAP機能を備える。

図28は、本発明における第6の実施例の端末1の構成例を示す。  
25 第1の実施例の端末1の機能に加えて、ホストOS13がMobile IPv6処理部252を備える。またゲストOS17は、Mobile IPv6処理部

25の代わりにHMIPv6処理部251を備える。

図29は、MAP3が送信するルータ広告のメッセージフォーマット例S4を示す。

ルータ広告メッセージを含むICMPパケット431は、IPv6パケット  
5 のペイロード部43に格納される。MAP3が送信するルータ広告S4は、MAPオプション432を含む。MAPオプション432は、HMIPv6対応端末の位置登録モードとMAPアドレスを端末に通知にする機能を持つ。

MIPv6対応端末の位置登録モードは、MAPオプション432のI、P、  
10 Vの各ビットの値によって3つのタイプに分類される。

タイプ1は、端末1がHA4との間で送受信する位置登録メッセージ（Binding Update、 Binding Acknowledgement）をMN-MAP間でカプセル化転送する方法である。

タイプ2は、端末1がHA4にBinding Updateを直接送信し、HA4  
15 から端末1へのBinding AcknowledgementをMAP-MN間でカプセル化転送する方法である。

タイプ3は、端末1がHA4との間で送受信する位置登録メッセージをHA4との間で直接送受信する方法である。

図31から図33に示すシーケンスに従って、図27に示す網5bに在  
20 圈するMN1がHA4に位置登録を行い、パケットを送受信するシーケンスを説明する。

まず、図31を用いて、上記タイプ1を示すルータ広告メッセージを受信したMN1のパケット送受信シーケンスを説明する。

MN1は、ルータ広告601を受信して、RCoAとLCoAを生成後、イ  
25 ンタフェース18にLCoAを設定する。次に、MN1は、MAP3bに位置登録メッセージ（Binding Update）を送信する（602）。MAP3bは、

RCoAとLCoAの対応情報を保持する。MAP3bは、上記Binidng Update  
に対する応答 (Binidng Acknowledgement) を送信する (603)。  
HMIPv6処理部251は、Binidng Update List管理テーブルを備え、  
上記テーブルにMAPのエントリを追加 (すでにエントリが存在す  
5 る場合は更新) する(604)。

次に、HMIPv6処理部251は、Binidng Acknowledgementにタイプ  
1のMAP位置登録であることを示す識別子を含むヘッダを追加し、  
シナリオ処理部23へ送信する(605、606)。

シナリオ処理部23は、BA処理ルーチン60を起動して、シナリオ  
10 を決定する(601、607)。

シナリオ処理部23は、RCoA、LCoA、MAPアドレスを受信パケッ  
トから取得する。MAPアドレスは送信元アドレス41aから、RCoA  
はIPv6 Routing Headerから、LCoAは着信先アドレス41bから、そ  
れぞれ取得する(95)。RCoAに変更があれば(96)、Mobility  
15 Header402のMobility Optionsにタイプ1のMAP位置登録を示す  
値を設定する。シナリオ処理部23は、上記Mobility Optionsを含  
むBinidng AcknowledgementをIPパケット処理部22経由でホスト  
OSのMobile IPv6処理部252に送信し(97、608、609)、本ルーチン  
を終了する。

20 RCoAに変更がなければ、本ルーチンを終了する。ステップ95  
で処理が正常に終了しなければ、受信パケットを廃棄し(67)、  
本ルーチンを終了する。

Mobile IPv6処理部252は、上記Binidng Acknowledgementを受  
信すると、HA4にBinidng Updateメッセージ(610)を送信する。

25 上記メッセージは、送信元アドレス41aにRCoAを、着信先アド  
レス41bにHA4アドレスを、Destination Options HeaderのHome

Address OptionにMN1のホームアドレスを設定する。上記メッセージ610を受信したHMIPv6処理部251は、上記パケットをIPinIPでカプセル化した後、MAP3b経由でHA4に送信する。

- HA4からBinidng Acknowledgement(611)を受信したMAP3bは
- 5 IPinIPカプセル化を行い、MN1にパケットを送信する。HMIPv6処理部251は上記メッセージを受信するとデカプセル化を行い、Mobile IPv6処理部252に送信する。上記メッセージには、送信元アドレス41aにHA4のアドレスが、着信先アドレス41bにRCoAが、Routing HeaderのHome AddressフィールドにMN1のホームアドレ
- 10 スが、それぞれ設定される。

上記位置登録信号のIPsec処理は、Mobile IP処理部252が行う。

- 次にMN1がパケットを送受信する方法を述べる。MN1が送受信するパケットに対して、Mobile IPv6処理部がMN1-HA4間のカプセル化・デカプセル化を行う。さらにHMIPv6処理部251がMN1-MAP
- 15 間のカプセル化・デカプセル化を行う(612、613)。

次に、図32を用いて、上記タイプ2を示すルータ広告メッセージを受信したMN1のパケット送受信シーケンスを説明する。

ステップ601から604は、図31の処理と同様である。

- 次に、HMIPv6処理部251は、Binidng Acknowledgementにタイプ
- 20 2のMAP位置登録であることを示す識別子を含むヘッダを追加し、シナリオ処理部23へ送信する(605、606)。

シナリオ処理部23は、BA処理ルーチン60を起動して、シナリオを決定する(61、607)。

- シナリオ処理部23は、RCoA、LCoA、MAPアドレスを受信パケッ
- 25 トから取得する。MAPアドレスは送信元アドレス41aから、RCoAはRouting Headerから、LCoAは着信先アドレス41bから、それぞ

れ取得する(98)。

RCoAに変更があれば(96)、Mobility Header402のMobility Optionsにタイプ2のMAP位置登録を示す値を設定する。シナリオ処理部23は、上記Mobility Optionsを含むBinidng AcknowledgementをIPパケット処理部22経由でホストOSのMobile IPv6処理部252に送信し(97、608、609)、本ルーチンを終了する。

RCoAに変更がなければ、本ルーチンを終了する。ステップ98で処理が正常に終了しなければ、受信パケットを廃棄し(67)、本ルーチンを終了する。

10 Mobile IPv6処理部252は、上記Binidng Acknowledgementを受信すると、HA4にBinidng Updateメッセージ(621)を送信する。

上記メッセージは、送信元アドレス41aにRCoAを、着信先アドレス41bにHA4アドレスを、Destination Options HeaderのHome Address OptionにMN1のホームアドレスを設定する。上記メッセージ621を受信したHMIPv6処理部251は、上記パケットをHA4に送信する。

HA4からBinidng Acknowledgement(622)を受信したMAP3bはIPinIPカプセル化を行い、MN1にパケットを送信する。HMIPv6処理部251は上記メッセージを受信するとデカプセル化を行い、20 Mobile IPv6処理部252に送信する。上記メッセージの送信元アドレス41aにはHA4のアドレスが、着信先アドレス41bにはRCoAが、Routing HeaderのHome AddressフィールドにはMN1のホームアドレスが、それぞれ設定される。

上記位置登録信号のIPsec処理は、Mobile IP処理部252が行う。

25 次にMN1のパケット受信方法(623)は、図31のステップ612と同様である。

MN1がパケットを送信する際、Mobile IPv6処理部252がMN-HA間カプセル化を行い、パケットを送信する(624)。

次に、図33を用いて、上記タイプ3を示すルータ広告メッセージを受信したMIPv6対応MN1のパケット送受信シーケンスを説明する。

ステップ601から604は、図31の処理と同様である。

次に、HMIPv6処理部251は、Binidng Acknowledgementにタイプ3のMAP位置登録であることを示す識別子を含むヘッダを追加し、シナリオ処理部23へ送信する(605、606)。

10 シナリオ処理部23は、BA処理ルーチン60を起動して、シナリオを決定する(61、607)。

シナリオ処理部23は、RCoA、LCoA、MAPアドレスを受信パケットから取得する。MAPアドレスは送信元アドレス41aから、RCoAはRouting Headerから、LCoAは着信先アドレス41bから、それぞれ取得する(99)。

RCoAに変更があれば(96)、Mobility Header402のMobility Optionsにタイプ3のMAP位置登録を示す値を設定する。シナリオ処理部23は、上記Mobility Optionsを含むBinidng AcknowledgementをIPパケット処理部22経由でホストOSのMobile IPv6処理部252に送信し(97、608、609)、本ルーチンを終了する。

RCoAに変更がなければ、本ルーチンを終了する。ステップ99で処理が正常に終了しなければ、受信パケットを廃棄し(67)、本ルーチンを終了する。

Mobile IPv6処理部252は、上記Binidng Acknowledgementを受信すると、HA4にBinidng Updateメッセージ(631)を送信する。

上記メッセージは、送信元アドレス41aにLCoAを、着信先アド

レス41bにHA4アドレスを、Destination Options HeaderのHome Address OptionにRCoAを、Binding UpdateのMobility OptionsのAlternate-care of address Optionフィールドに、MN1のホームアドレスを設定する。上記メッセージ631を受信したHMIPv6処理部251は、上記パケットをHA4に送信する。

HA4からBinding Acknowledgement (632)を受信したHMIPv6処理部251は上記メッセージをMobile IPv6処理部252に送信する。上記メッセージの送信元アドレス41aにはHA4のアドレスが、着信先アドレス41bにはLCoAが、Routing HeaderのHome AddressフィールドにはMN1のホームアドレスが設定される。

上記位置登録信号のIPsec処理は、Mobile IPv6処理部252が行う。

次にMN1のパケット送受信方法(633、634)は、図32のステップ623、624と同様である。

本発明の第6の実施の形態によると、Mobile IPv6対応MNにHMIPv6サービスの提供が容易に実現できる。さらに、Mobile IPv6処理部とHMIPv6処理部を分離することにより、HMIPv6対応端末のIPinIPカプセル化处理、或いは、IPsec処理が容易になる。

(実施例7)

本発明の第7の実施の形態を図を用いて説明する。図34は、本発明における第7の実施例の通信網の構成例を示す。第7の実施例は、ルータ3(3a、3b)にMobile Router10(10a、10b)が接続され、各Mobile Router10がMobile Network9(9a、9b)を構成することを特徴とする。

図35は、MN1のホーム網6に設置するHA4の構成例を示す。HA4は、回線(318a、318b、318m、318n)を収容するインタフェース

部 (IF) (319a、319b、319m、319n) と、サーバ部311 (311a、311b、311m) と、スイッチ部317 (317a、317b) から構成される。

サーバ部311は、パケット受信・送信処理部313と、IPsec処理部314と、Mobile IP処理部315とを備える。

- 5      Mobile IP処理部315は、Mobile IPプロトコル処理機能と、Mobile IPのホームエージェント (HA) 機能を備える。Mobile IPのホームエージェント機能は、Binding Cache管理テーブルを備える。Binding Cache管理テーブルは、MN1のホームアドレスと気付アドレスの対応情報を保持する。さらに、本実施例における
- 10    HA4は、Mobile IP処理部315に、モバイルトンネル処理を複数回実行する処理プログラムを備える。

図36は、HA4が、Mobile Router10、および、Mobile Network9内のMN1のHAである場合のモバイルトンネル適用区間を示す。

- HA4がMN1と通信する場合、MN1とHA4の間 ((1)MN-HAモバイルトンネル) と、Mobile Router10とHA4の間 ((2)MR-HAモバイルトンネル) に、モバイルトンネルを設定する。
- 15

- まず、HA4は、MN1のバインディング情報を参照して、オリジナルパケット351にIPヘッダ352を追加する。IPヘッダ352の着信先アドレスには、MN1の気付アドレス (CoA) が設定される。次にHA4
- 20    は、Mobile Router (MR) 10のバインディング情報を参照して、IPヘッダ353を追加する。IPヘッダ353の着信先アドレスには、MR10の気付アドレスが設定される。

- 本発明の第7の実施の形態によると、HA4がNetwork Mobilityサービス提供時に必要な複数回のIPinIPカプセル化处理、或いは、
- 25    IPsec処理が容易に実現できる。

(実施例8)

本発明の第 8 の実施の形態を図を用いて説明する。図38は、本発明における第 8 の実施例の通信網の構成例を示す。第 8 の実施例は、MN1のホーム網6とCN2を含むネットワーク 361が、GW362を介して、IP網7に接続されることを特徴とする。GW362は、TLS終  
5 端機能を備える。

第 8 の実施例において、MN1のゲストOS APL16は第 1 のTLS終端機能を備える。MN1のホストOS APL11が第 2 のTLS終端機能を備える。

図39は、MN 1 がTLSを用いて通信を行う場合のシーケンスを説  
10 明する。

ネットワーク 361の外部に存在するMN 1 が、ネットワーク 361に存在する通信装置（CN2）と通信を行う場合、MN1とGW362の間にTLSを設定して通信を行う。

まず、MN1とGW362の間にTLSのセッションを設定する手順を説明  
15 する。MN1のゲストOS APL16が、利用可能な暗号アルゴリズム、圧縮アルゴリズム、クライアントランダム値等を含むClient HelloメッセージをGW362に送信する（701）。上記メッセージを受信したGW362は、利用する暗号アルゴリズムと圧縮アルゴリズムを決定する。次にGW362は、決定した値とサーバランダム値を  
20 含むServer HelloメッセージをMN1のゲストOS APL16に通知する（702）。GW362は、必要に応じて自身の証明書等を送付してもよい。GW362がMN1に証明書を送付すると、MN1は、上記証明書を用いて、GW362の認証を行うことが可能になる。GW362は、オプションメッセージの送信終了をServer Hello DoneでMN1のゲストOS APL16  
25 に通知する（703）。MN 1 のゲストOS APL16は、各暗号パラメータのタネとなるプリマスタシークレットを生成して、Client Key

ExchangeメッセージでGW362 に通知する (704) 。

- ここで、MN1のゲストOS APL16とGW362は、利用アルゴリズム、サーバランダム、クライアントランダム、プリマスタシーケツトを共有した状態となる。MN1のゲストOS APL16とGW362は、暗号化通信に必要なセキュリティパラメータを生成する。

MN1のゲストOS APL16とGW362は、セキュリティパラメータの設定終了 (Change Cipher Spec) と新しい暗号化仕様の動作の確認 (Finished)をそれぞれ通知する (705から708)。以上で、MN1のゲストOS APL16とGW362の間にTLSのセッションが確立する (709)。

- 次に、MN1のホストOS APL11で動作するアプリケーションが、CN2との間でTLSを用いた通信712を行うため、メッセージを交換し (710)、MN1のホストOS APL11とCN2の間にTLSセッション711を確立する。TLSコネクション711の設定手順は、ステップ701から708と同様であるため、詳細は省略する。TLSセッション711は、MN1のゲストOS APL16とGW362の間のTLSセッション709を利用する。

本発明の第8の実施の形態によると、MN1がTLSセッションを2つの通信装置との間で確立する場合、複数回のTLS処理が容易に実現できる。

## 20 (実施例9)

本発明は、以下のような移動体端末装置でも実現される。

- 互いに接続された第一及び第二の網と、上記第一の網に接続されたホームエージェントとを備えた通信システムにおいて、該ホームエージェントに接続された移動体端末装置であって、該移動体端末から上記ホームエージェントに向けて送信された位置登録に対する上記ホームエージェントからの応答を受信し、該応答

から上記移動端末装置で用いる通信方式を決定することの特徴とする移動体端末装置。

または、

- 上記移動体端末装置は、Mobile IPv6処理部と、IPアドレス変換部を備え、上記移動体端末装置が第一のアドレス体系に従うパケットを受信したときは、上記Mobile IPv6処理部が、上記受信したパケットをMobile IPv6処理した後、上記IPアドレス変換部が、上記Mobile IPv6処理されたパケットを第二のアドレス体系に変換し、上記移動体端末装置が第一のアドレス体系に従うパケットを送信するときは、上記IPアドレス変換部が、上記送信するパケットを第二のアドレス体系に変換した後、上記Mobile IPv6処理部が、上記変換されたパケットをMobile IPv6処理すること
- 10      を特徴とする上記移動体端末装置。

または、

- 15      上記第一のアドレス体系がIPv6であり、上記第二のアドレス体系がIPv4であることを特徴とする上記移動体端末装置。

または、

- 上記移動体端末装置は、Mobile IPv6処理部と、第一のIPsec処理部を備え、上記Mobile IPv6処理部は、さらにその内部に第二のIPsec処理部を備え、上記移動体端末装置がパケットを受信したときは、上記第二のIPsec処理部が、上記受信したパケットに対して、Mobile IPv6処理に関するIPsec処理を行った後、上記第一のIPsec処理部が、上記IPsec処理されたパケットに対して、さらにIPsec処理を行うことを特徴とする上記移動体端末装置。
- 20      上記移動体端末装置は、Mobile IPv6処理部と、第一のIPsec処理部を備え、上記Mobile IPv6処理部は、さらにその内部に第二のIPsec処理部を備え、上記移動体端末装置がパケットを受信したときは、上記第二のIPsec処理部が、上記受信したパケットに対して、Mobile IPv6処理に関するIPsec処理を行った後、上記第一のIPsec処理部が、上記IPsec処理されたパケットに対して、さらにIPsec処理を行うことを特徴とする上記移動体端末装置。

- 25      または、

上記通信システムはさらに、上記第一及び第二の網を接続する

接続装置を備え、上記接続装置はHMIPv6のMAPであることを特徴とする上記移動体端末装置。

(産業上の利用可能性)

- 本発明を用いると、通信装置は、同一レイヤのセキュリティ処理、
- 5 又は、ヘッダ処理を複数回終端することが可能になる。本発明は、セキュリティ管理形態に応じた処理を行う通信装置を実現する場合に利用される可能性がある。

## 請求の範囲

1. ネットワークに接続され、パケットを送信及び受信する送受信部と、CPUと、上記送受信部から受信したパケットに対して上記CPUが行う第一及び第二の処理用のプログラムを記憶したメモリとを備えた端末であって、上記第一の処理及び第二の処理は、上記受信したパケットの同じレイヤに対する処理であることを特徴とする端末。
2. 上記第一及び第二の処理は、上記受信したパケットの同じレイヤに対する終端処理であることを特徴とする請求項1記載の端末。
3. 上記第一及び第二の処理は、上記受信したパケットの同じレイヤに施されたセキュリティ処理を終端する処理であることを特徴とする請求項1または2記載の端末。
4. 上記第一及び第二の処理は、上記受信したパケットの同じレイヤに施された暗号化を復号する処理であることを特徴とする請求項1乃至3のいずれかに記載の端末。
5. 上記第一及び第二の処理は、上記受信したパケットの同じレイヤに施されたIPsecの終端処理であることを特徴とする請求項1乃至4のいずれかに記載の端末。
6. 上記第一及び第二の処理は、上記受信したパケットの同じレイヤに施されたTLSの終端処理であることを特徴とする請求項1乃至4のいずれかに記載の端末。
7. 上記メモリにはさらに、第一のオペレーションシステム用のプログラム及び該第一のオペレーションシステム上で動作する第二のオペレーションシステム用のプログラムが記憶されてお

り、上記第一の処理は上記第二のオペレーションシステム上での処理であり、上記第二の処理は上記第一のオペレーションシステム上での処理であることを特徴とする請求項 1 乃至 6 のいずれかに記載の端末。

- 5    8. 上記第二のオペレーションシステムは、上記第一のオペレーションシステム上に構築された仮想マシン上で動作することを特徴とする請求項 7 記載の端末。

9. 上記ネットワークにはさらに、上記端末の位置情報を管理するサーバが接続されており、上記第一及び第二の処理の対象である上記受信されたパケットは、上記サーバから上記端末へ送信されたパケットであることを特徴とする請求項 1 乃至 8 のいずれかに記載の端末。
- 10

10. 上記端末及び上記サーバは Mobile IP の機能に対応した端末及びサーバであって、上記端末は Mobile Node
- 15    として機能する端末であり、上記サーバは、上記端末の Home Agent として機能するサーバであることを特徴とする請求項 9 記載の端末。

11. ネットワークに接続された端末及びサーバを備えた通信システムであって、上記端末は、パケットを送信及び受信する送受信部と、CPU と、上記送受信部から受信したパケットに対して上記 CPU が行う第一及び第二の処理用のプログラムを記憶したメモリとを備えた端末であって、上記サーバは、パケットを送信及び受信する送受信部と、CPU と、上記端末の位置情報を記憶したメモリとを備えたサーバであって、上記端末における第一
- 20
- 25    の処理及び第二の処理は、上記サーバから受信したパケットの同じレイヤに対する処理あることを特徴とする通信システム。

1 2. 上記端末における第一及び第二の処理は、上記受信したパケットの同じレイヤに対する終端処理であることを特徴とする請求項 1 1 記載の通信システム。

1 3. 上記端末における第一及び第二の処理は、上記受信したパケットの同じレイヤに施されたセキュリティ処理を終端する処理であることを特徴とする請求項 1 1 または 1 2 記載の通信システム。

1 4. 上記端末における第一及び第二の処理は、上記受信したパケットの同じレイヤに施された暗号化を復号する処理であることを特徴とする請求項 1 1 乃至 1 3 のいずれかに記載の通信システム。

1 5. 上記端末における第一及び第二の処理は、上記受信したパケットの同じレイヤに施されたIPsecの終端処理であることを特徴とする請求項 1 1 乃至 1 4 のいずれかに記載の通信システム。

1 6. 上記端末における第一及び第二の処理は、上記受信したパケットの同じレイヤに施されたTLSの終端処理であることを特徴とする請求項 1 1 乃至 1 4 のいずれかに記載の通信システム。

1 7. 上記端末のメモリにはさらに、第一のオペレーションシステム用のプログラム及び該第一のオペレーションシステム上で動作する第二のオペレーションシステム用のプログラムが記憶されており、上記端末における第一の処理は上記第二のオペレーションシステム上での処理であり、上記端末における第二の処理は上記第一のオペレーションシステム上での処理であることを特徴とする請求項 1 1 乃至 1 6 のいずれかに記載の通信システム。

1 8. 上記第二のオペレーションシステムは、上記第一のオペレ

ーションシステム上で構築された仮想マシン上で動作することを特徴とする請求項 17 記載の通信システム。

19. 上記端末及び上記サーバは Mobile IP の機能に対応した端末及びサーバであって、上記端末は Mobile Node  
5 として機能する端末であり、上記サーバは、上記端末の Home Agent として機能するサーバであることを特徴とする請求項 11 乃至 18 のいずれかに記載の通信システム。

20. ネットワークを介して端末またはルータに接続され、パケットを送信及び受信する送受信部と、CPU と、上記端末または  
10 上記ルータのアドレスを記憶したメモリを備えたホームエージェントであって、さらに上記送受信部から受信したパケットに対して上記 CPU が行う第一及び第二の処理用のプログラムを記憶したメモリを備え、上記第一の処理及び第二の処理は、上記受信したパケットの同じレイヤに対する処理であることを特徴とする  
15 するホームエージェント。

21. 移動端末と移動ルータに接続され、上記移動端末と上記移動ルータのアドレスを記憶した上記メモリを有し、上記移動端末から上記移動ルータを経由して受信したパケットに対して上記第一の処理及び第二の処理を行うことを特徴とする請求項 20  
20 記載のホームエージェント。

22. 上記第一及び第二の処理は、上記受信したパケットの同じレイヤに対する終端処理であることを特徴とする請求項 20 記載のホームエージェント。

23. 上記第一及び第二の処理は、上記受信したパケットの同じ  
25 レイヤに施されたセキュリティ処理を終端する処理であることを特徴とする請求項 20 記載のホームエージェント。

24. 上記第一及び第二の処理は、上記受信したパケットの同じレイヤに施された暗号化を復号する処理であることを特徴とする請求項20記載のホームエージェント。

5 25. 上記第一及び第二の処理は、上記受信したパケットの同じレイヤに施されたIPsecの終端処理であることを特徴とする請求項20記載のホームエージェント。

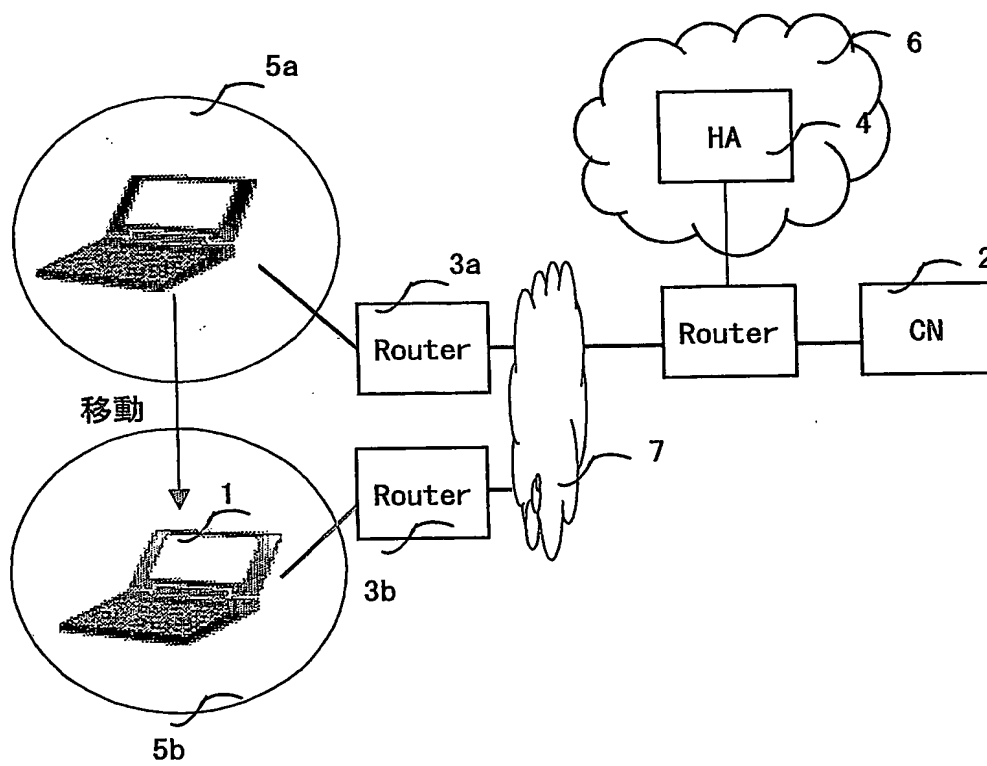
26. 上記第一及び第二の処理は、上記受信したパケットの同じレイヤに施されたTLSの終端処理であることを特徴とする請求項20記載のホームエージェント。

10 27. 上記プログラムを記憶したメモリはさらに、第一のオペレーションシステム用のプログラム及び該第一のオペレーションシステム上で動作する第二のオペレーションシステム用のプログラムが記憶されており、上記第一の処理は上記第二のオペレーションシステム上での処理であり、上記第二の処理は上記第一の  
15 オペレーションシステム上での処理であることを特徴とする請求項20記載のホームエージェント。

28. 上記第二のオペレーションシステムは、上記第一のオペレーションシステム上に構築された仮想マシン上で動作することを特徴とする請求項27記載のホームエージェント。

1/39

図1



2/39

図2

端末機能ブロック図

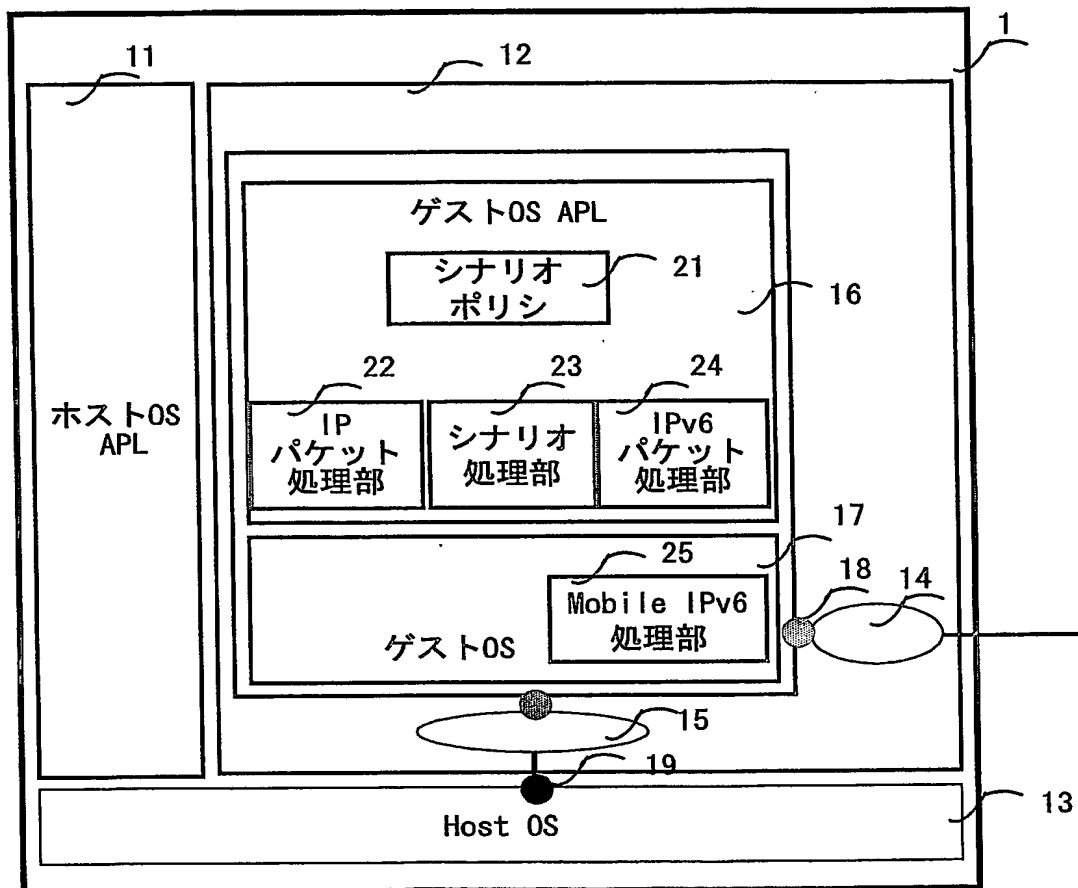


図3

210 Binding Update List管理テーブル

211 BU送信先 アドレス	212 Home Address	213 Care of Address	214 Lifetime	
				210-1
				210-2
				210-n

4/39

図4

220 シナリオポリシー管理テーブル

221 シナリオ番号	222 シナリオ内容	223 状態
10000	IPv4-IPv6変換有 (IPsecなし)	off 221-1
10001	IPv4-IPv6変換無 (IPsecなし)	off 221-2
10010	IPv4-IPv6変換有	off 221-3
10011	IPv4-IPv6変換有 経路最適化有	off 221-4
11000	IPv4-IPv6変換無	off 221-5
11000	IPv4-IPv6変換無 経路最適化有	off 221-6
10100	MAP タイプ1	off 221-7
10200	MAP タイプ2	off 221-8
10300	MAP タイプ3	off 221-9

5/39

図5

端末機能ブロック図

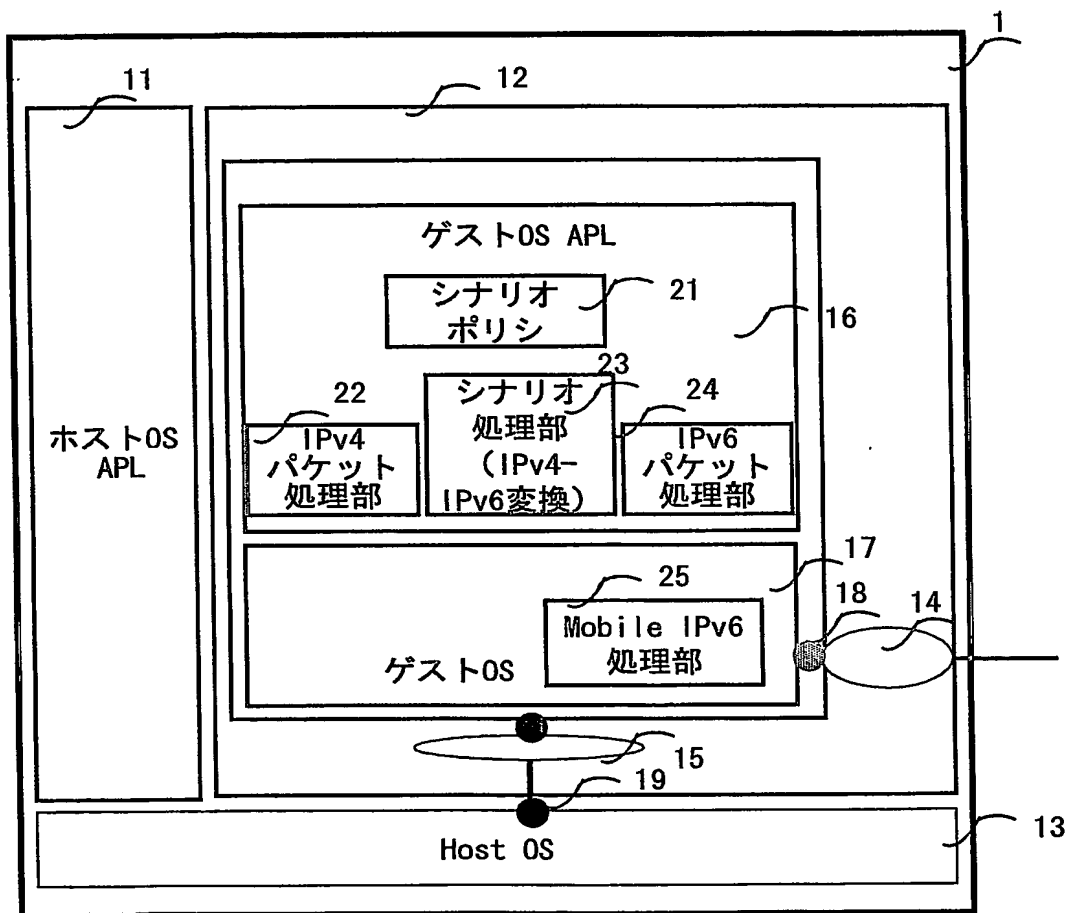


図6

230    IPv4－IPv6変換テーブル

231 IPv6	232 IPv4	233 Lifetime
2000:0:0:7::1000 (HoAv6)	192.168.0.10 (HoAv4)	xxx
2000:0:0:8::1001 (CN v6)	192.168.0.100 (CN仮想v4)	yyy

図7

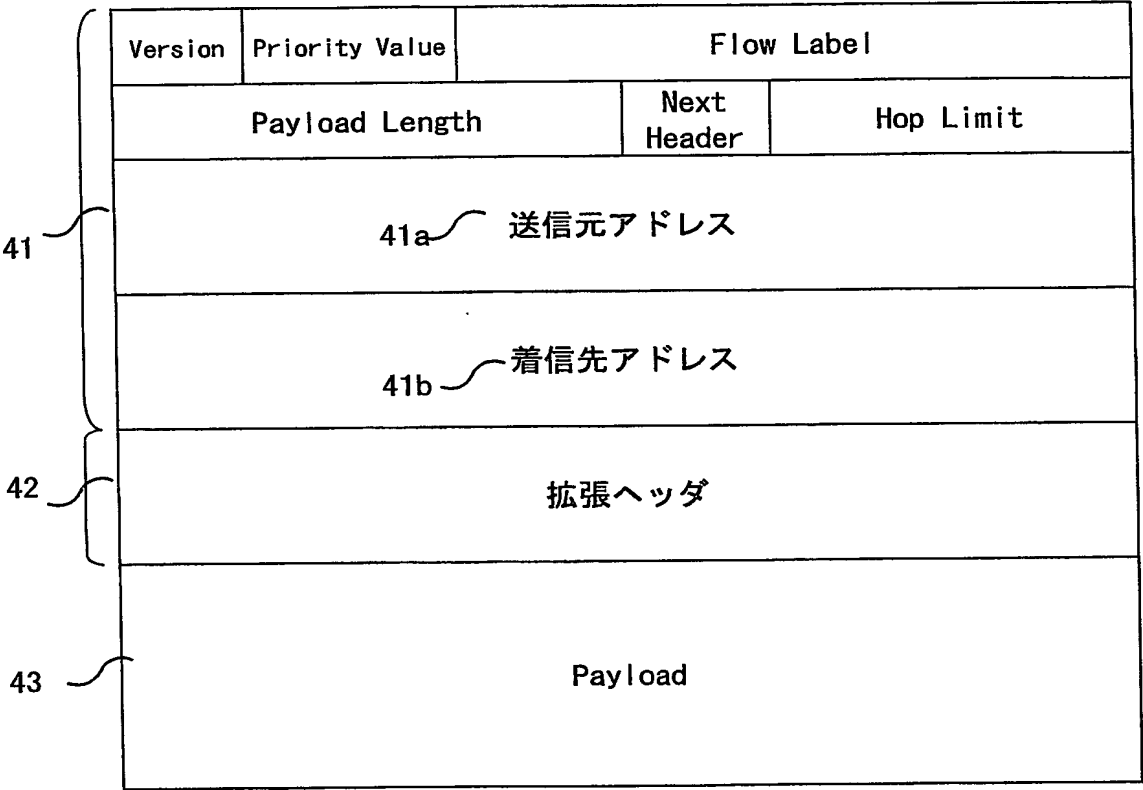


図8

S1 Binding Acknowledgementメッセージフォーマット

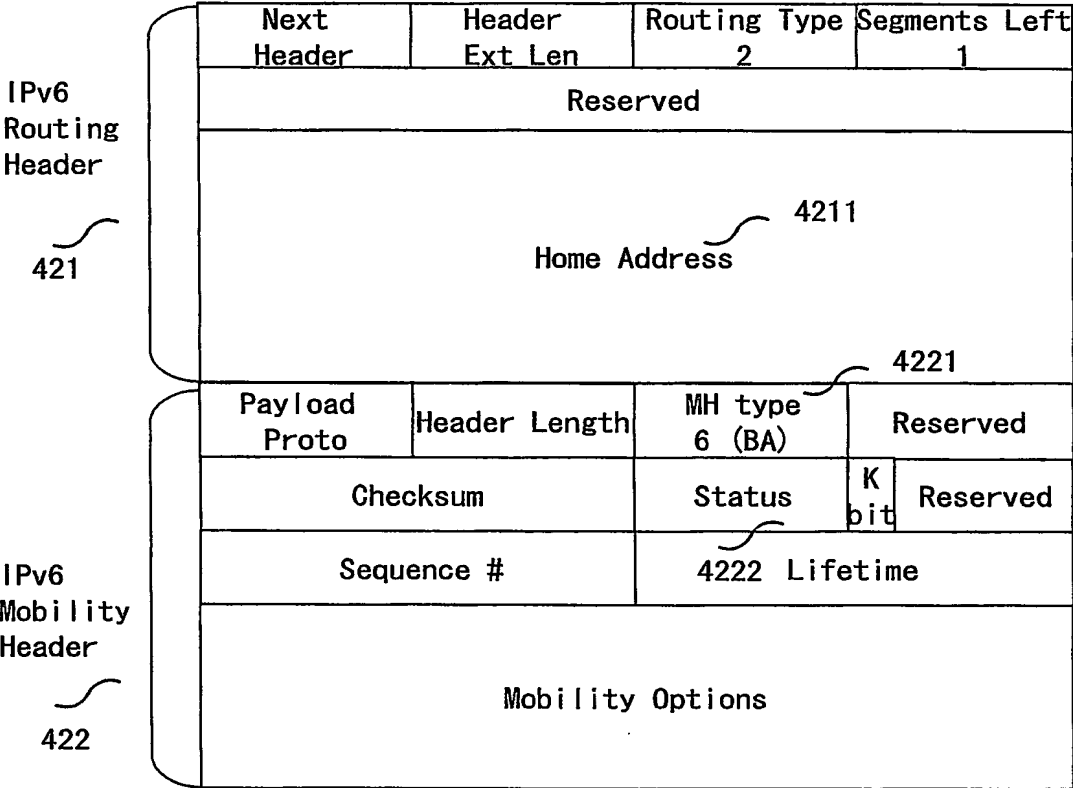
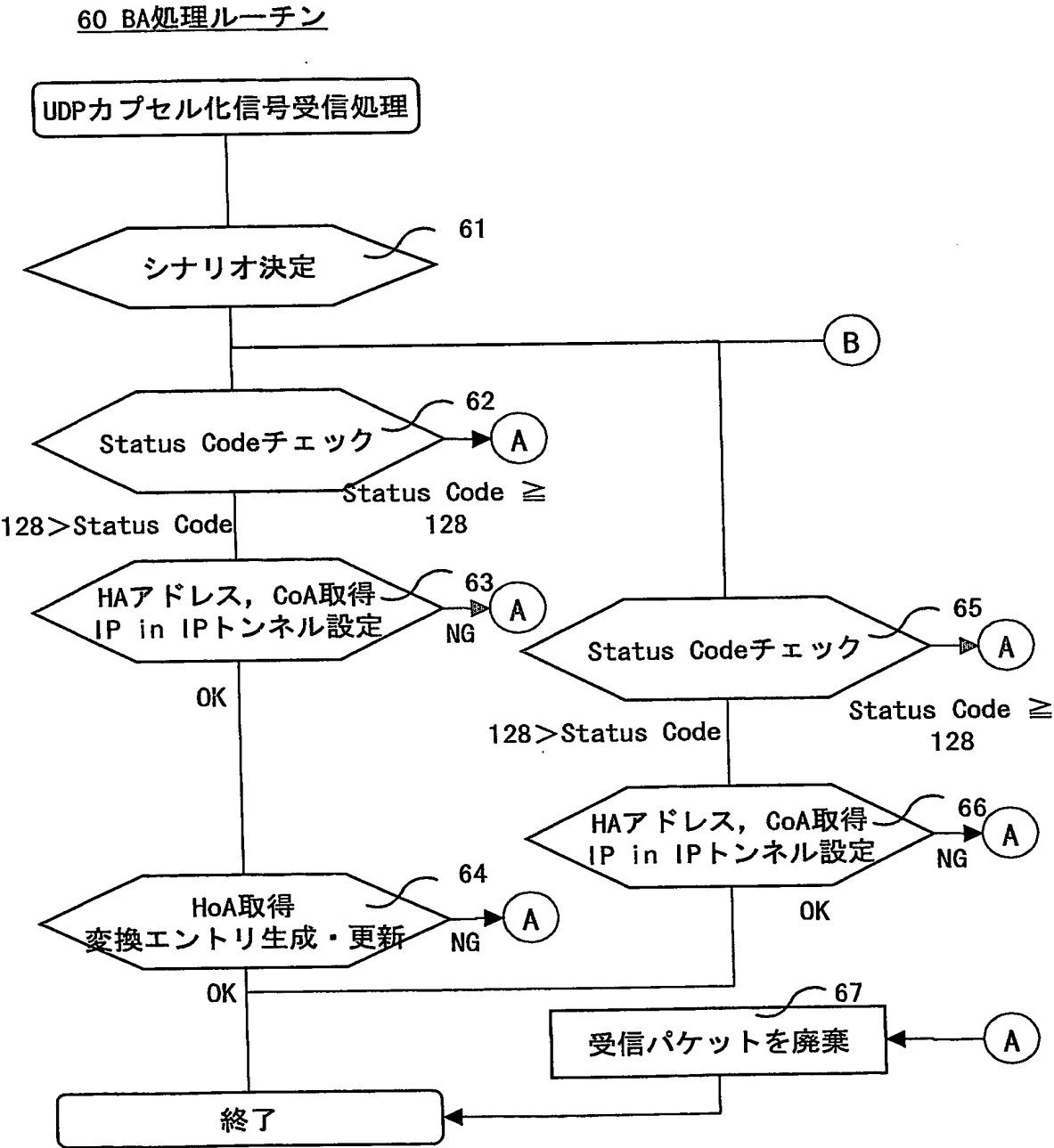


図9



10/39

図10

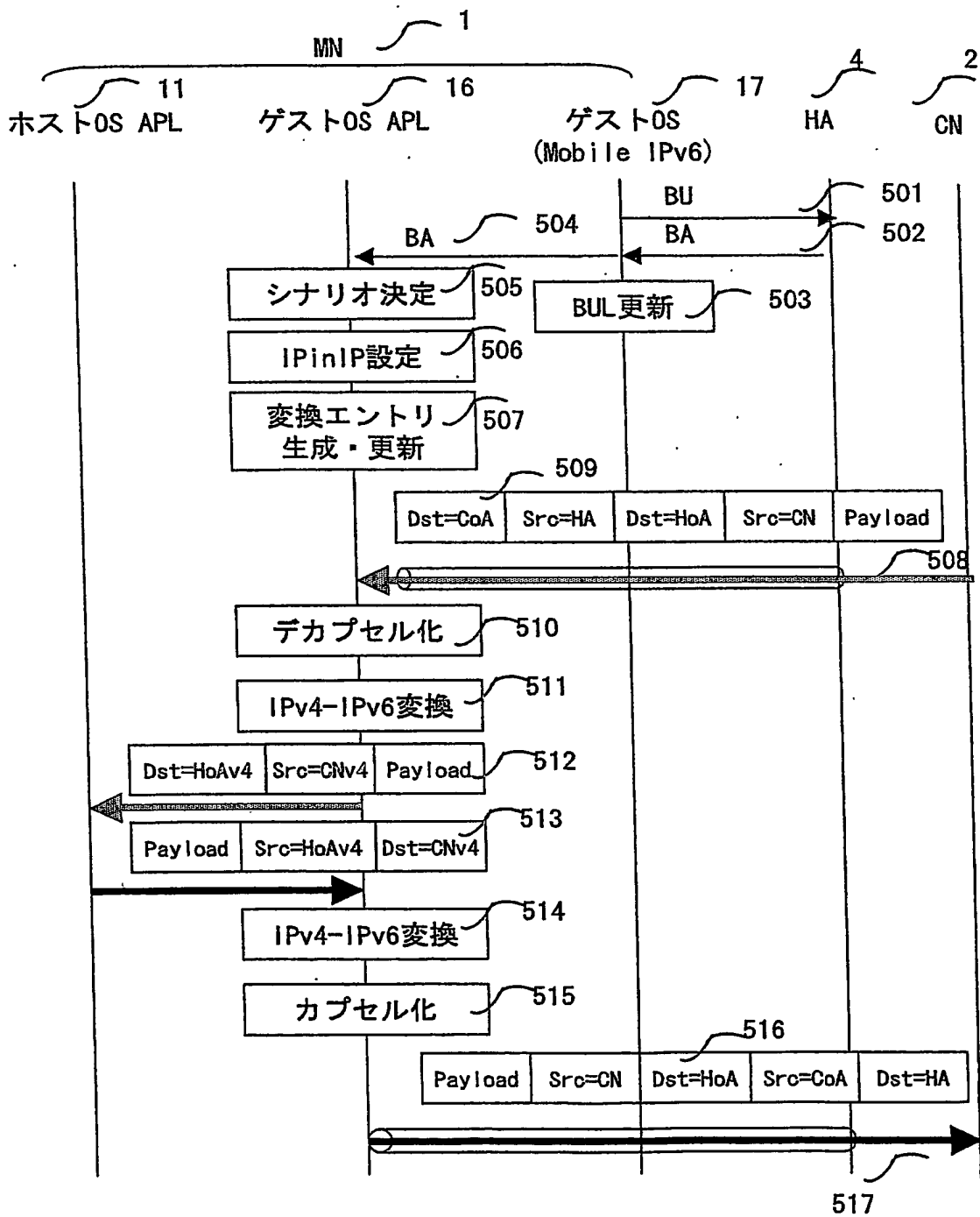
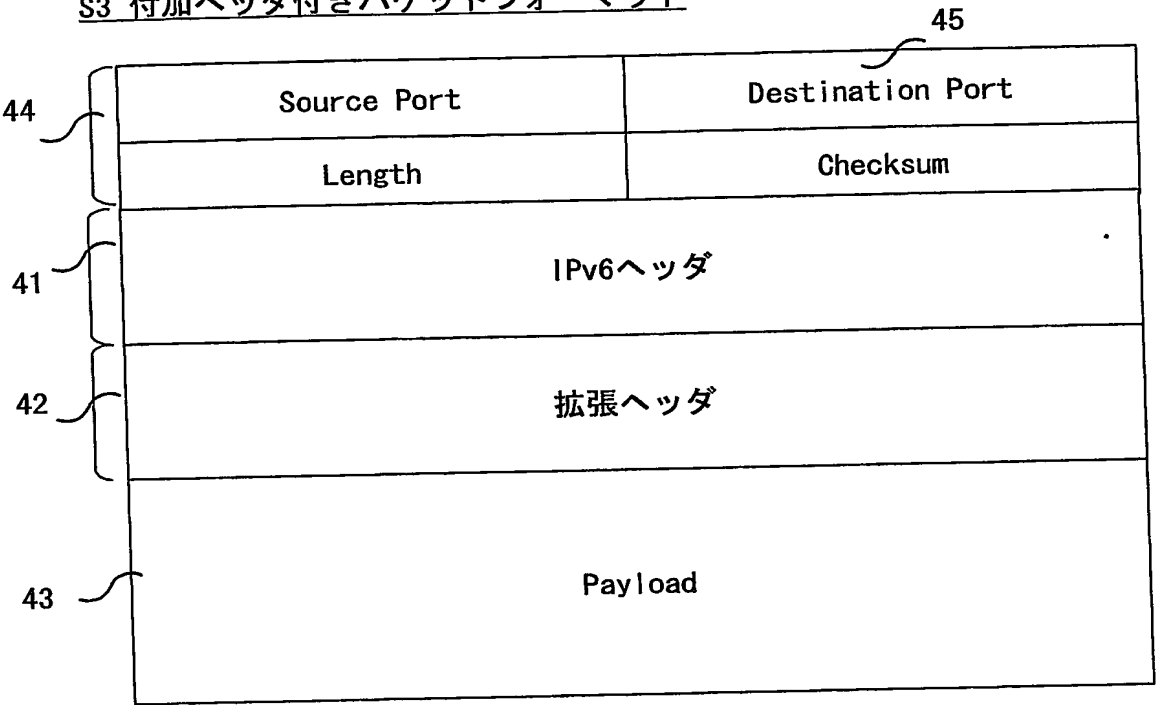


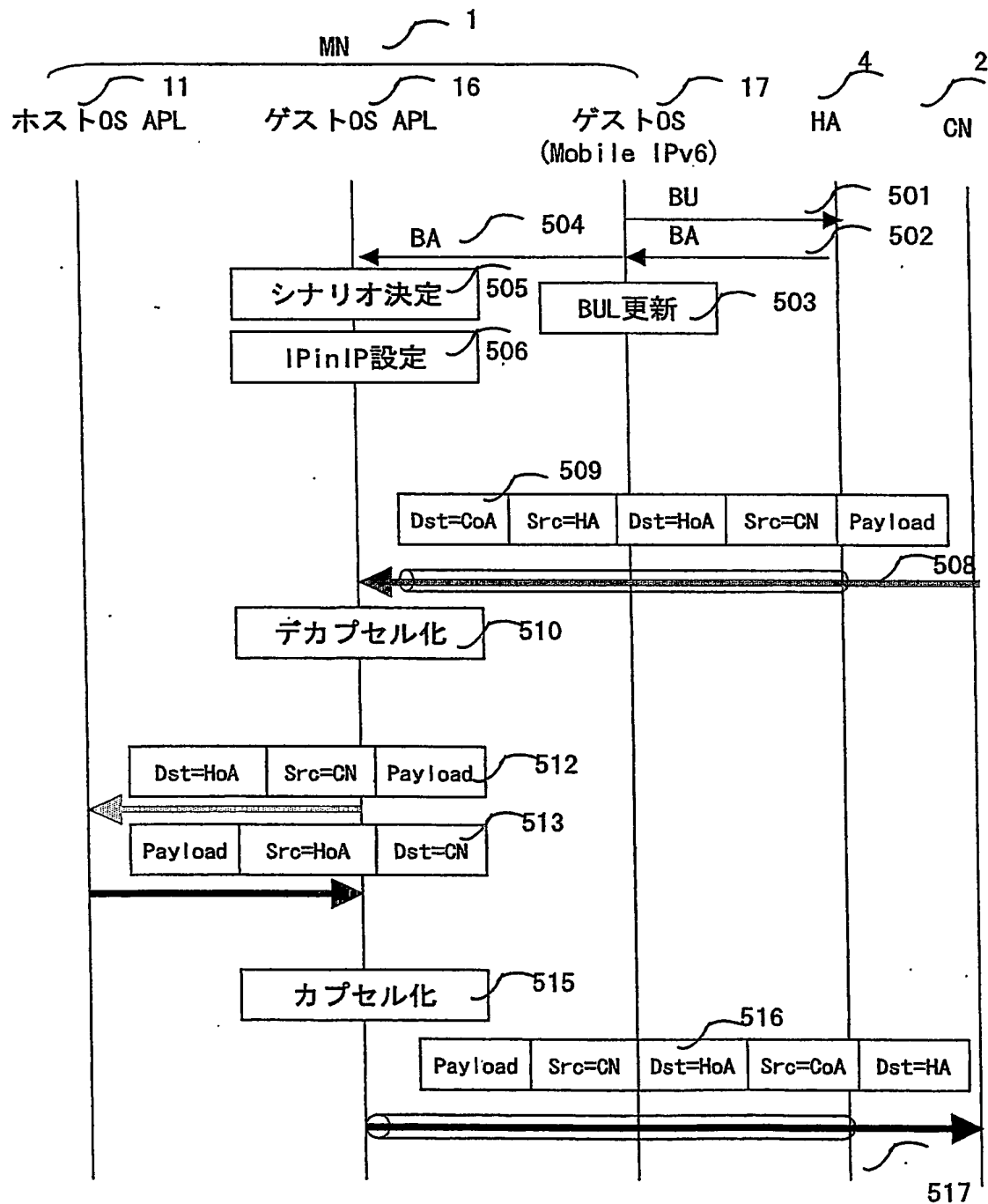
図11

S3 付加ヘッダ付きパケットフォーマット



12/39

図12



13/39

図13

## 70 BA処理ルーチン (MIPv6処理部)

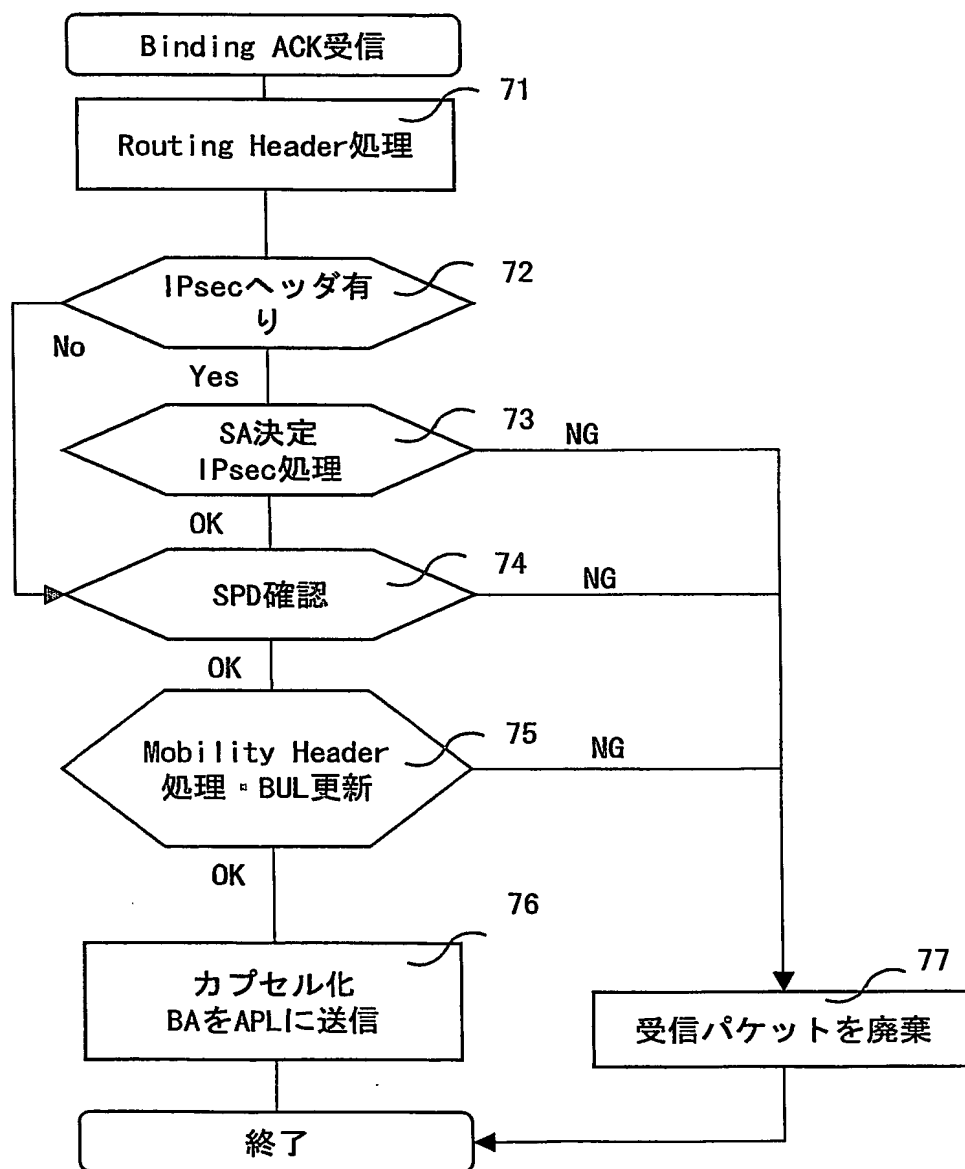
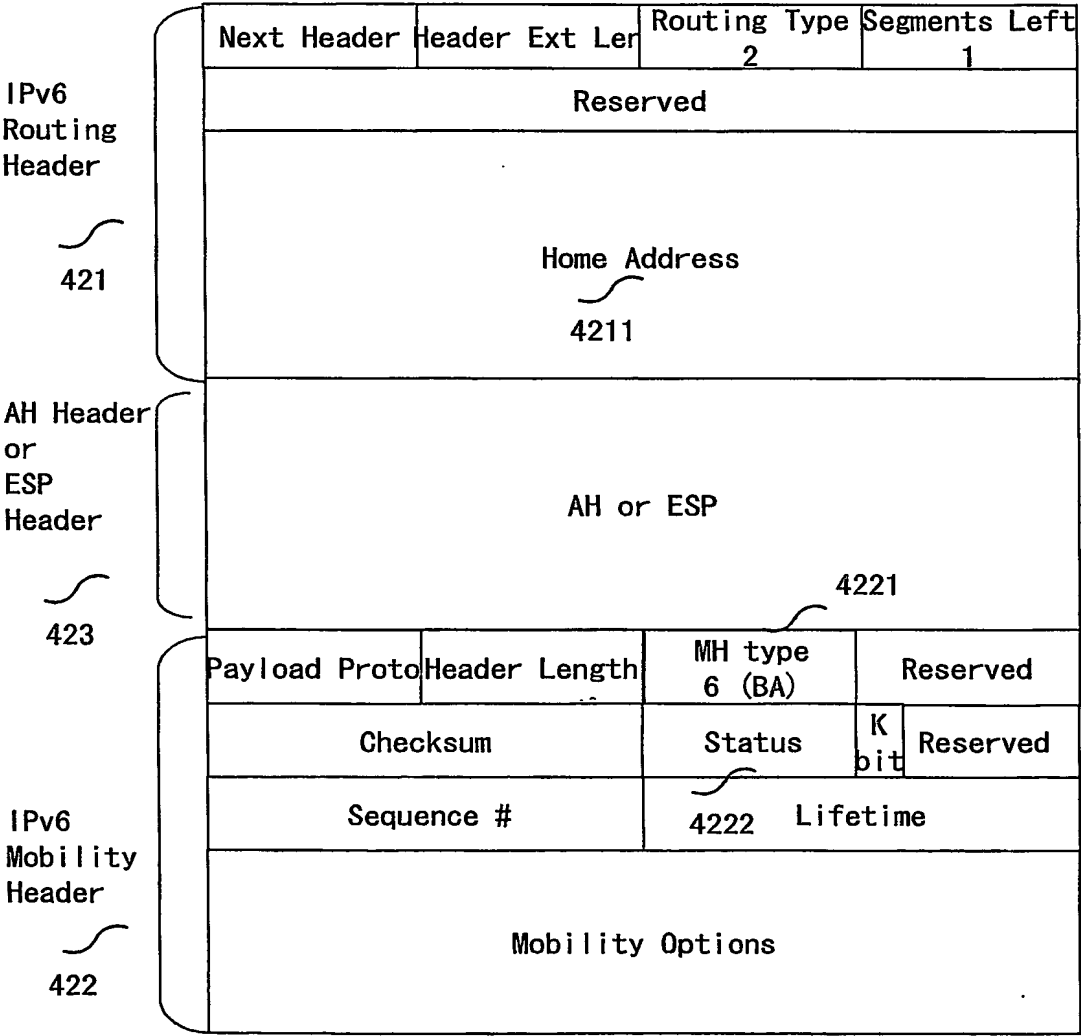


図14

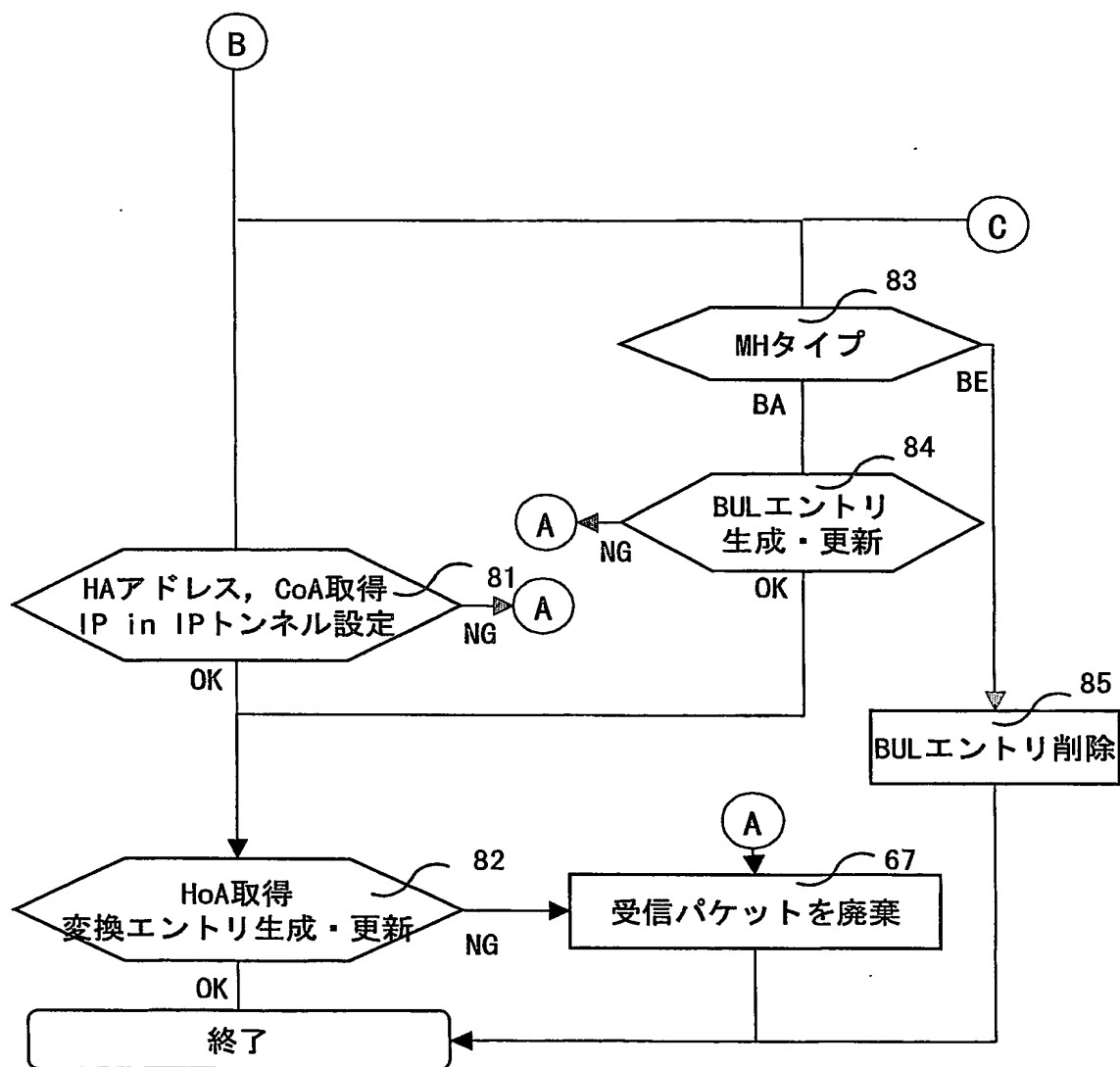
S2 Binding Acknowledgementメッセージフォーマット



15/39

図15

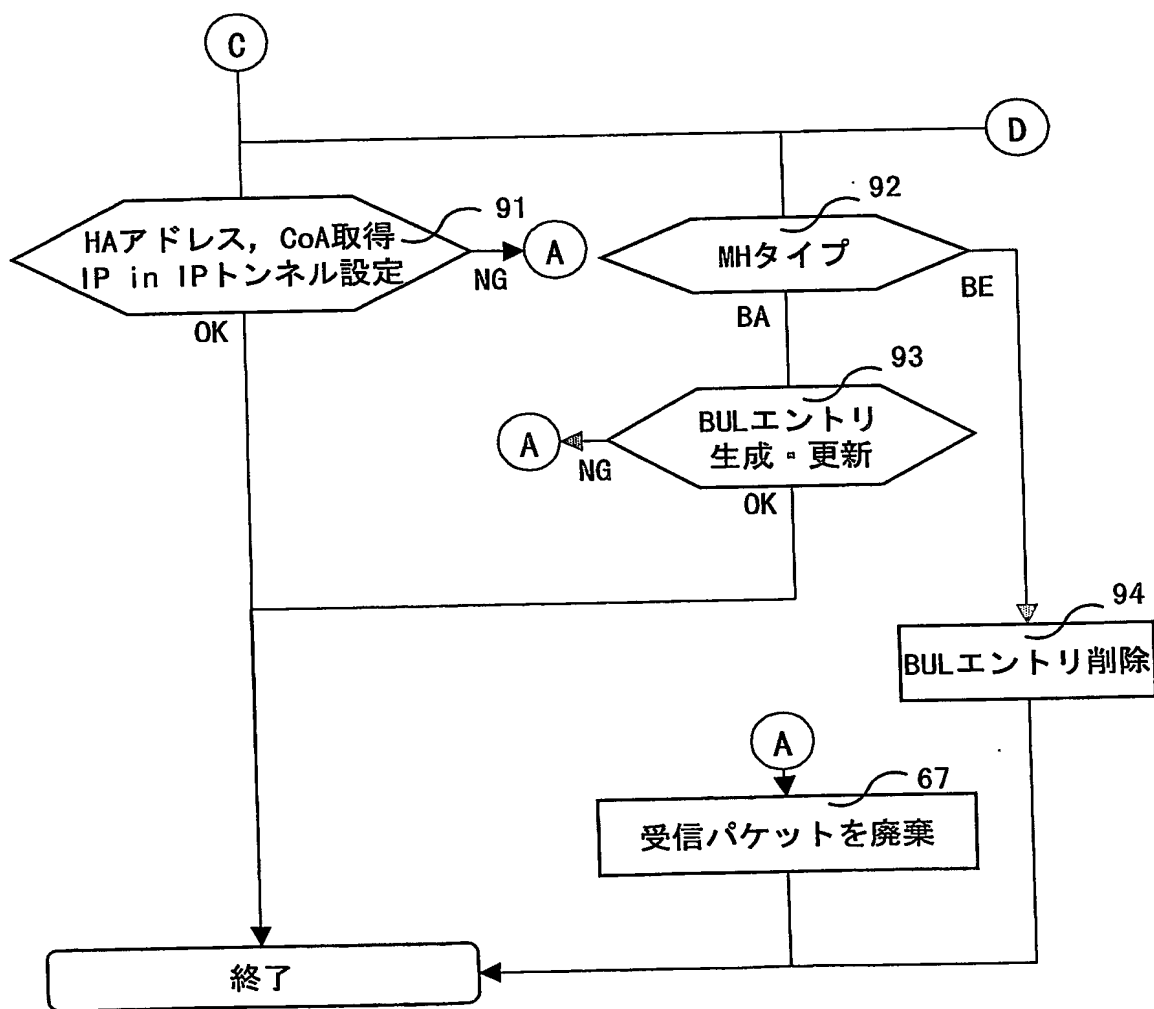
## 60 BA処理ルーチン



16/39

図16

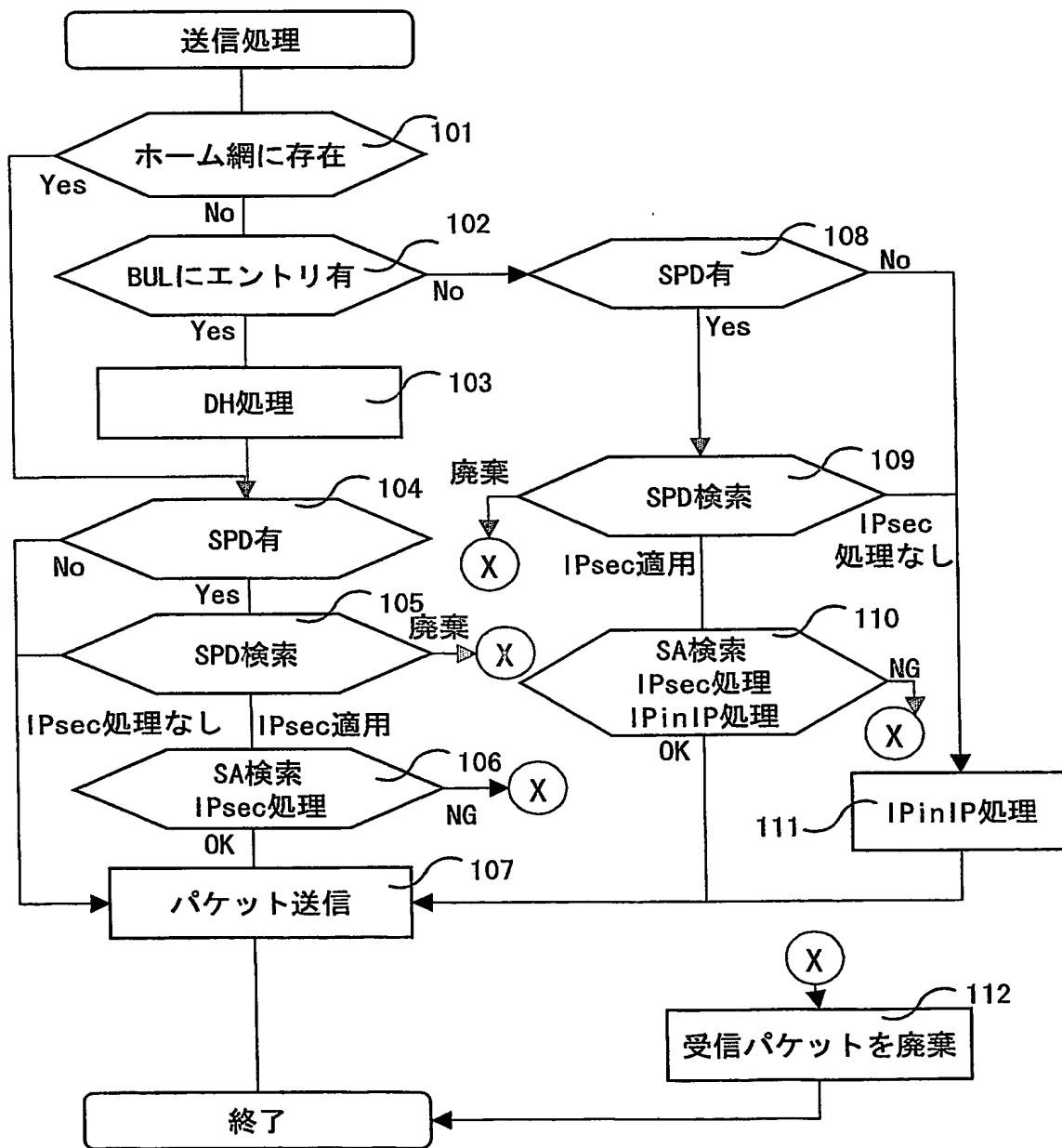
## 60 BA処理ルーチン



17/39

図17

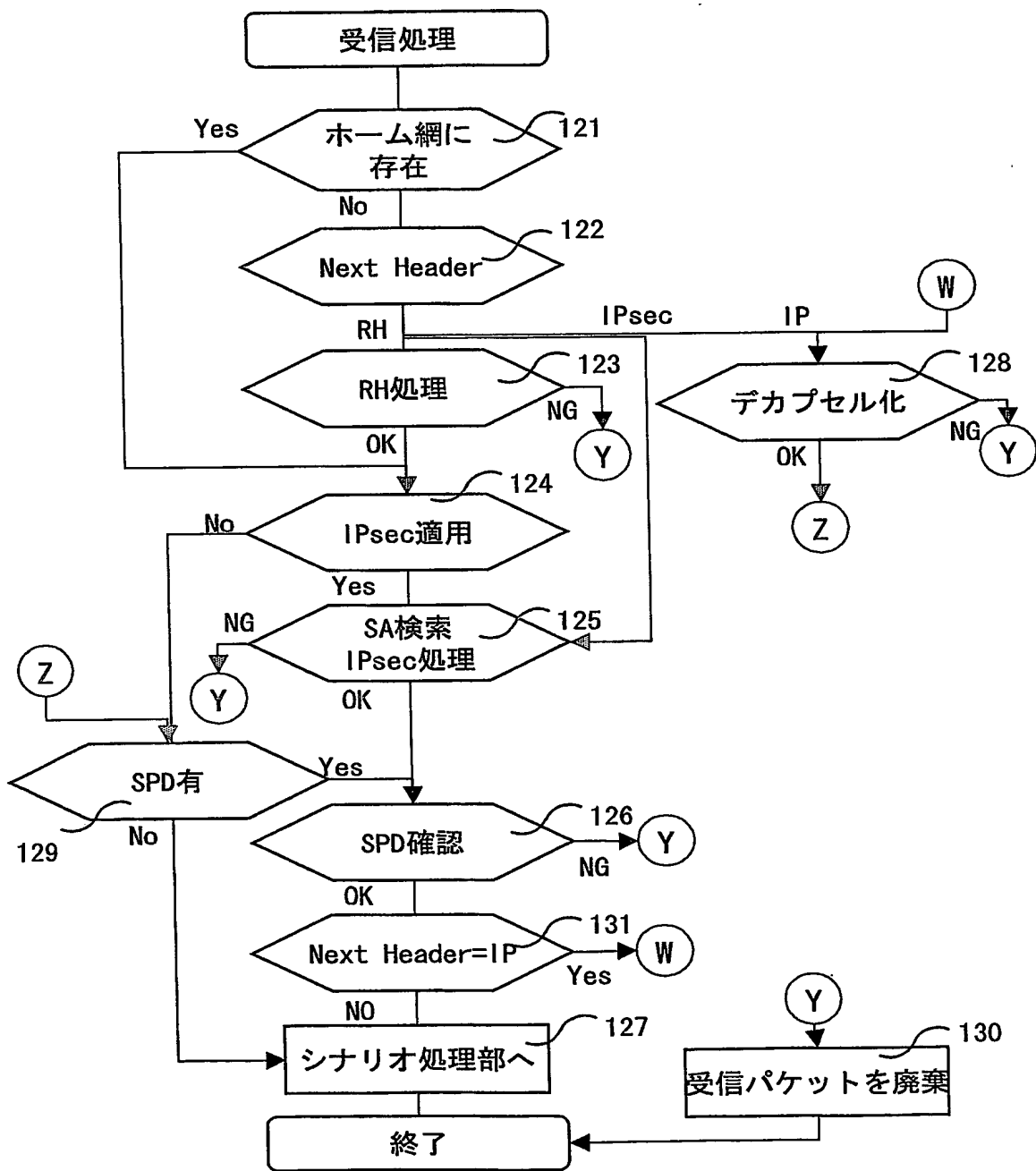
## 100 パケット送信処理ルーチン (ゲストOS APL)



18/39

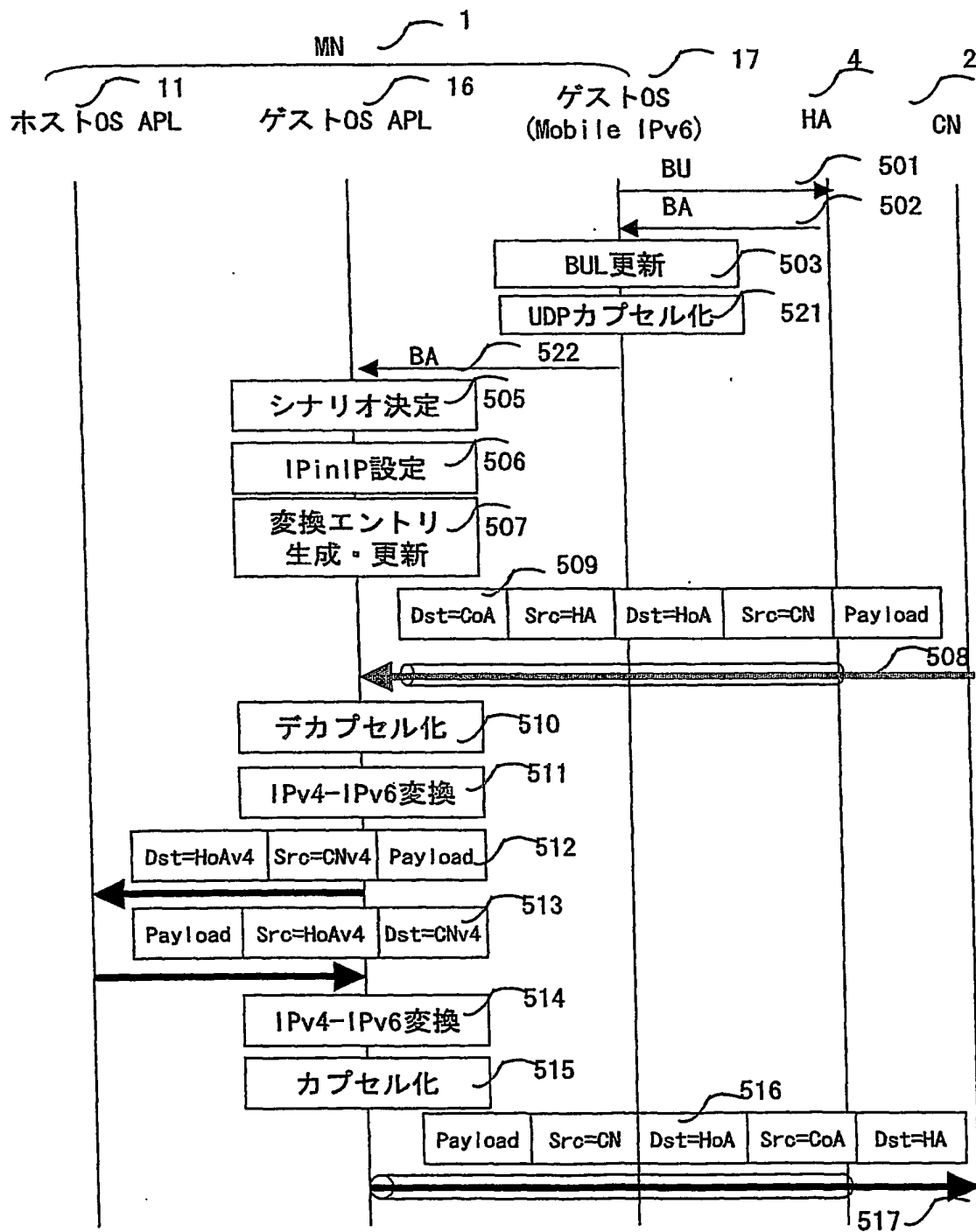
図18

## 120 パケット受信処理ルーチン (ゲストOS APL)



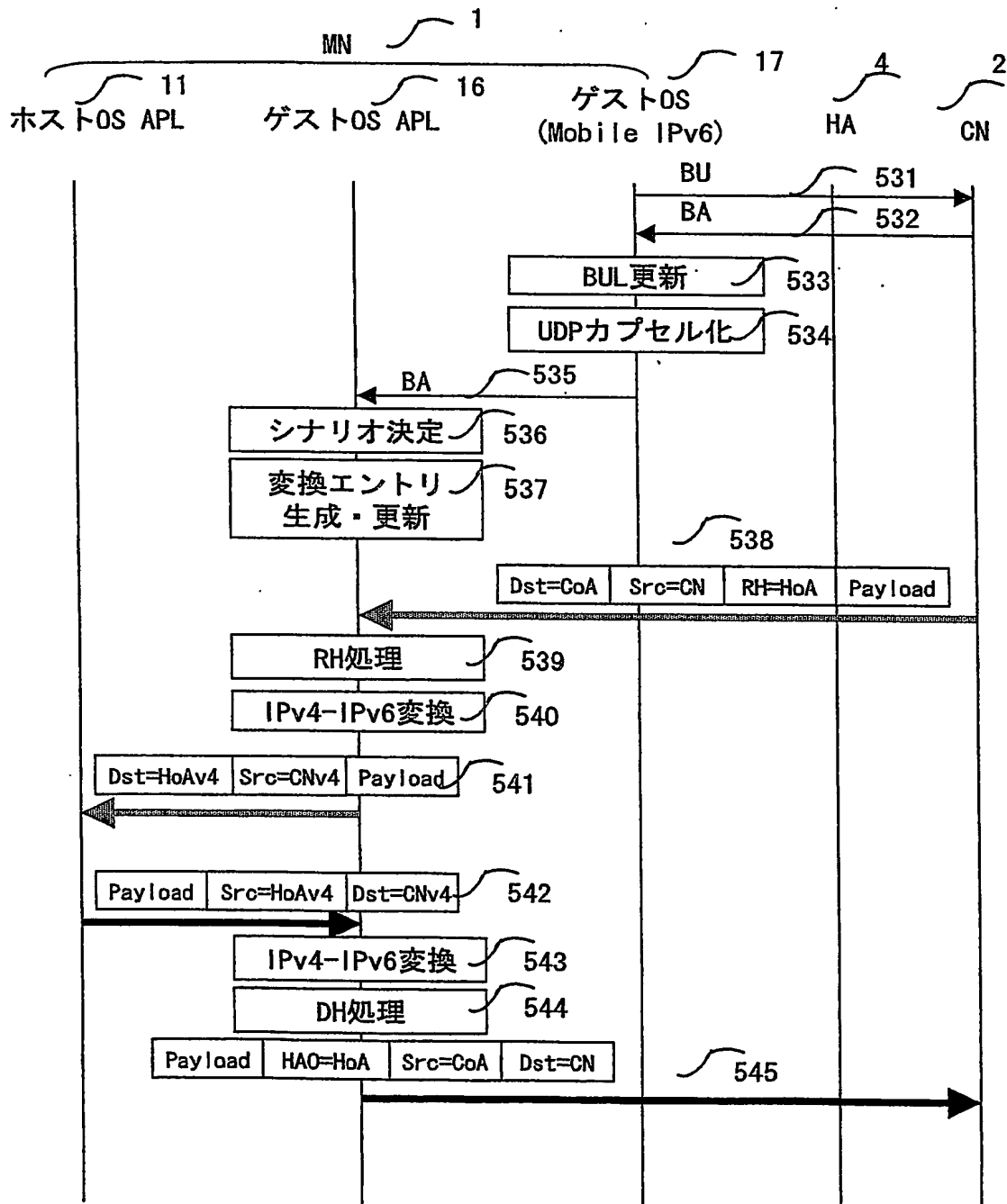
19/39

図19



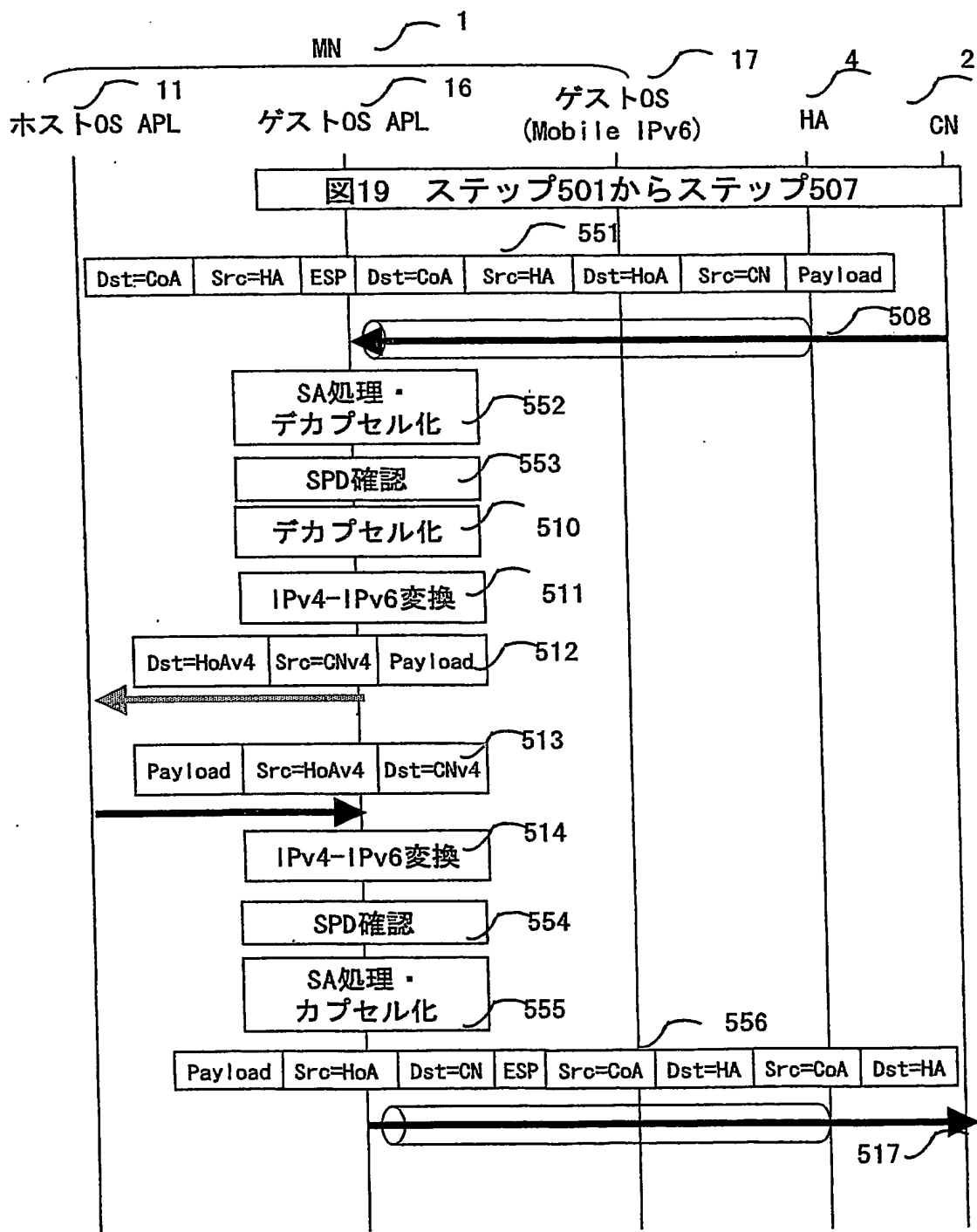
20/39

図20



21/39

図21



22/39

図22

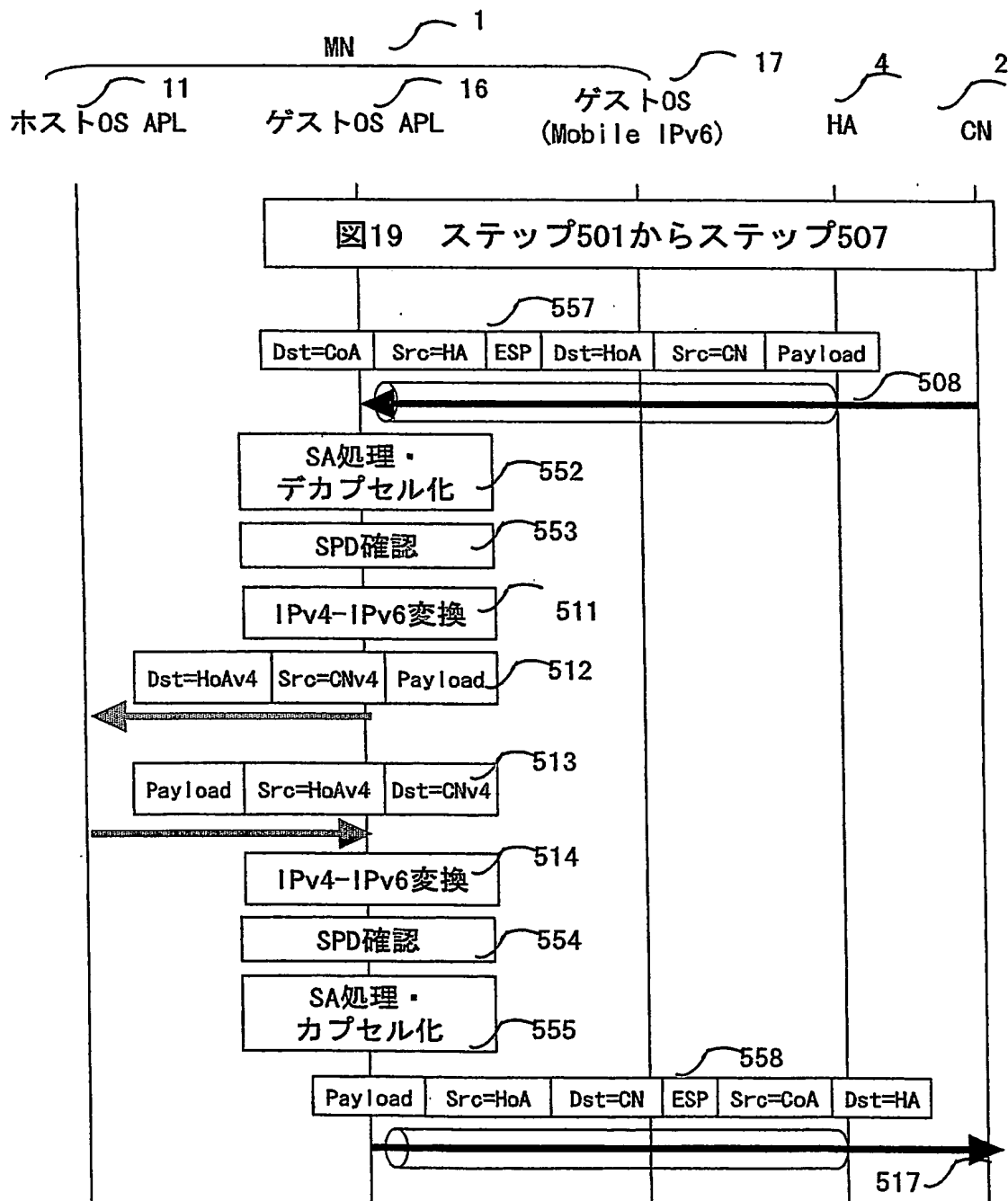
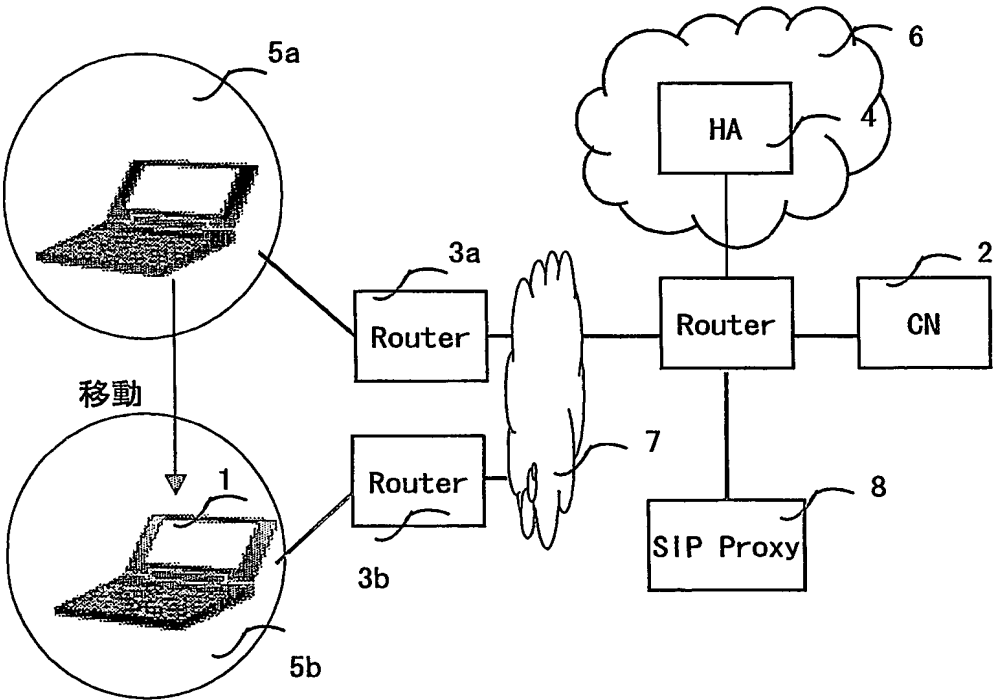


図23



24/39

図24

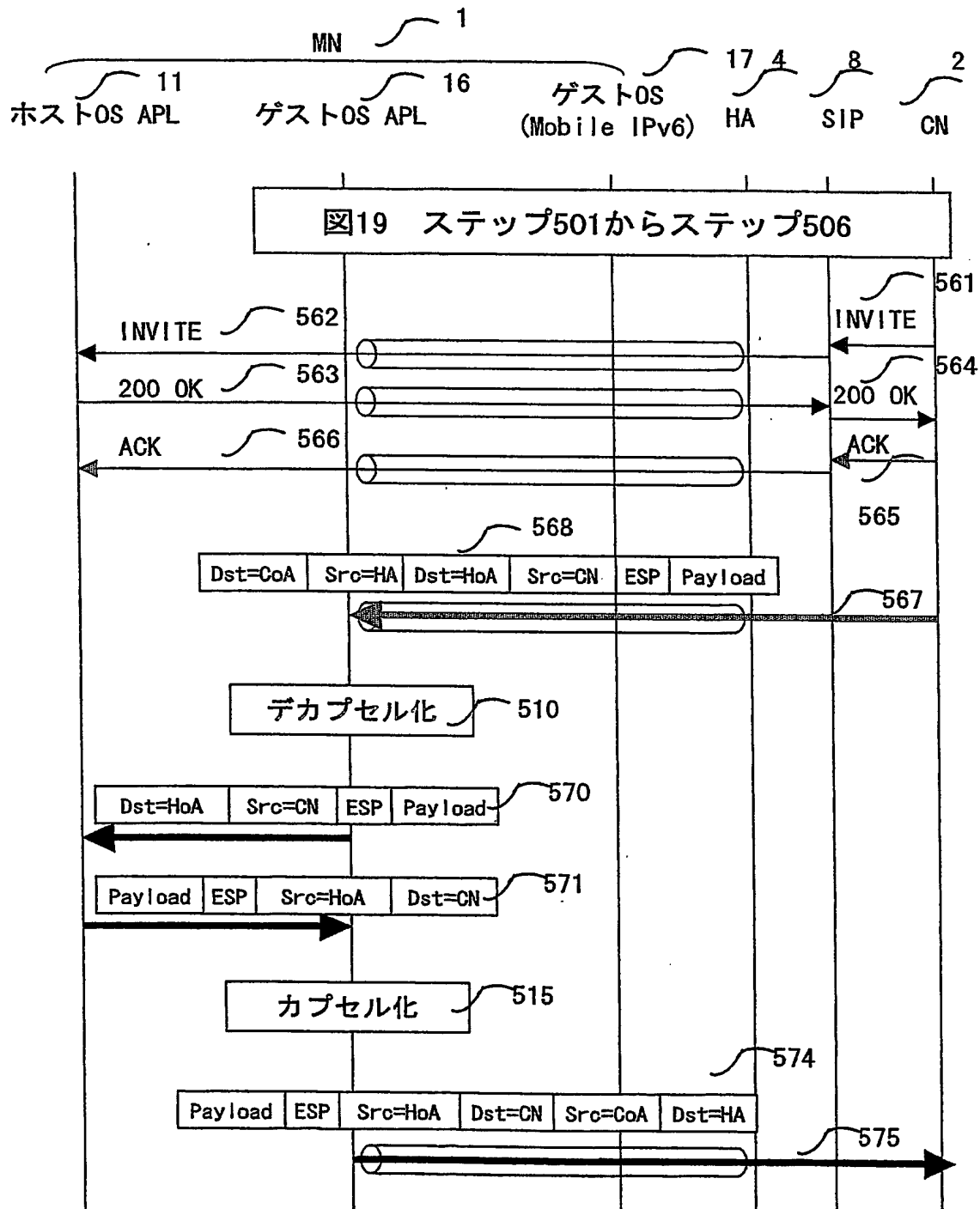


図25

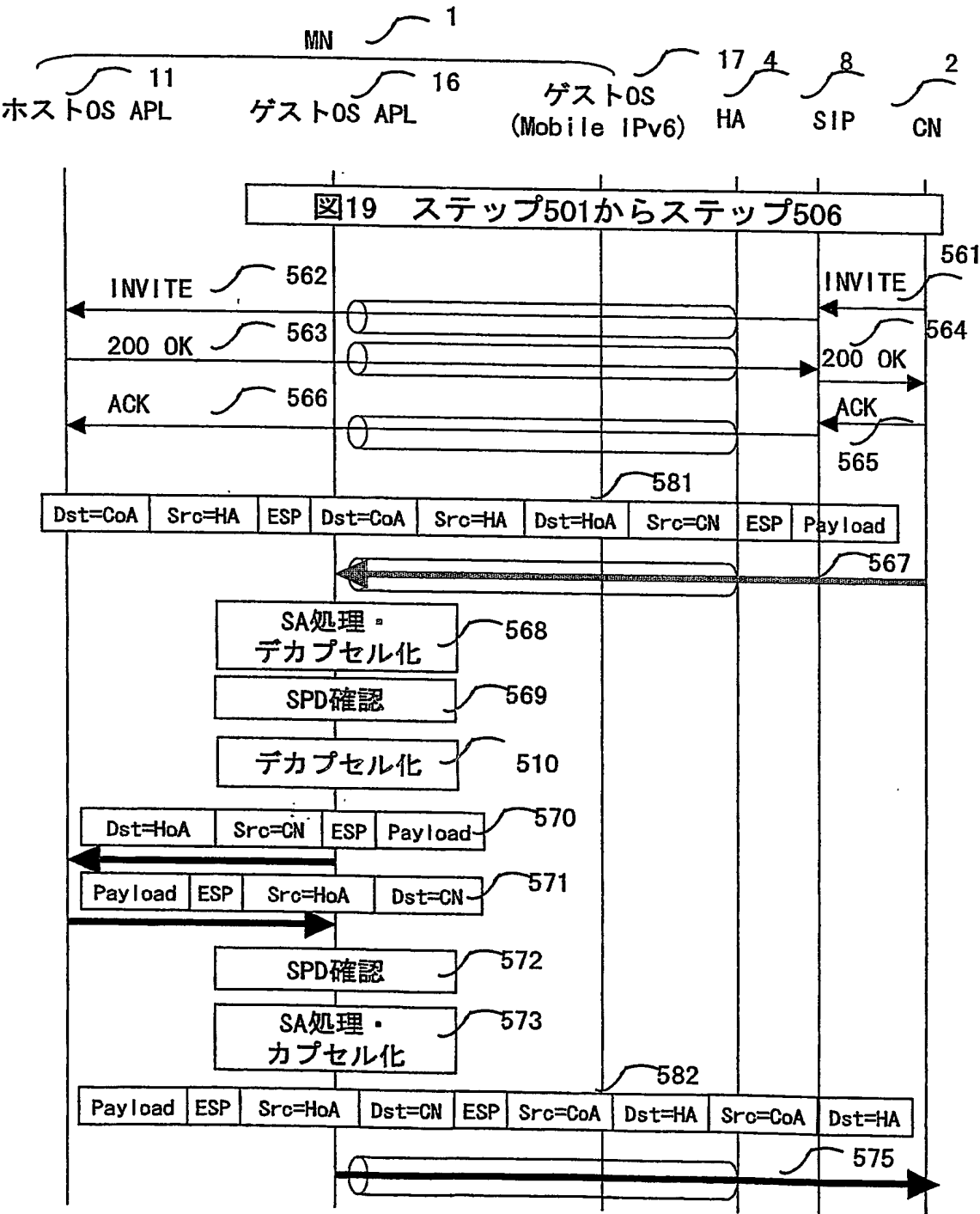
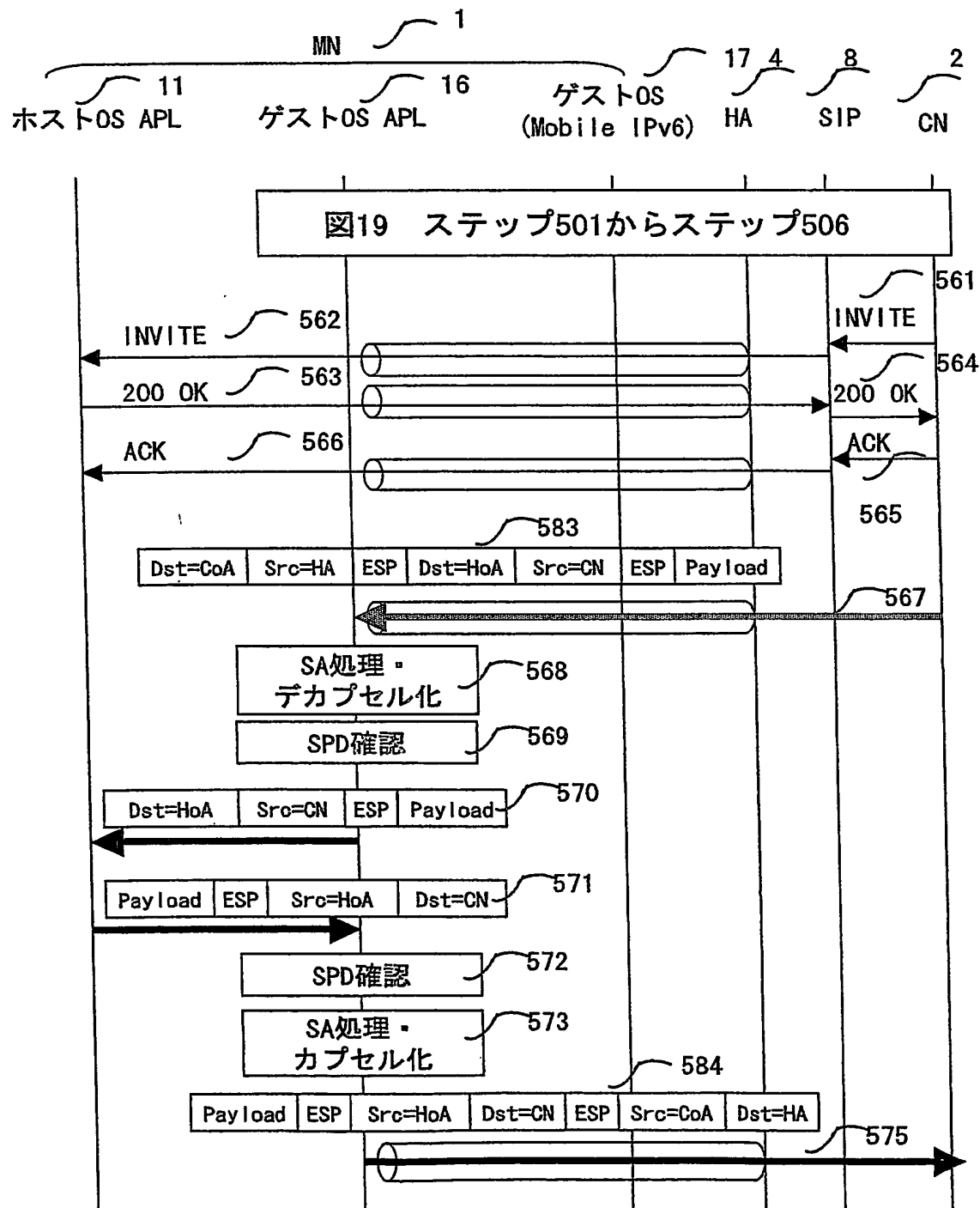
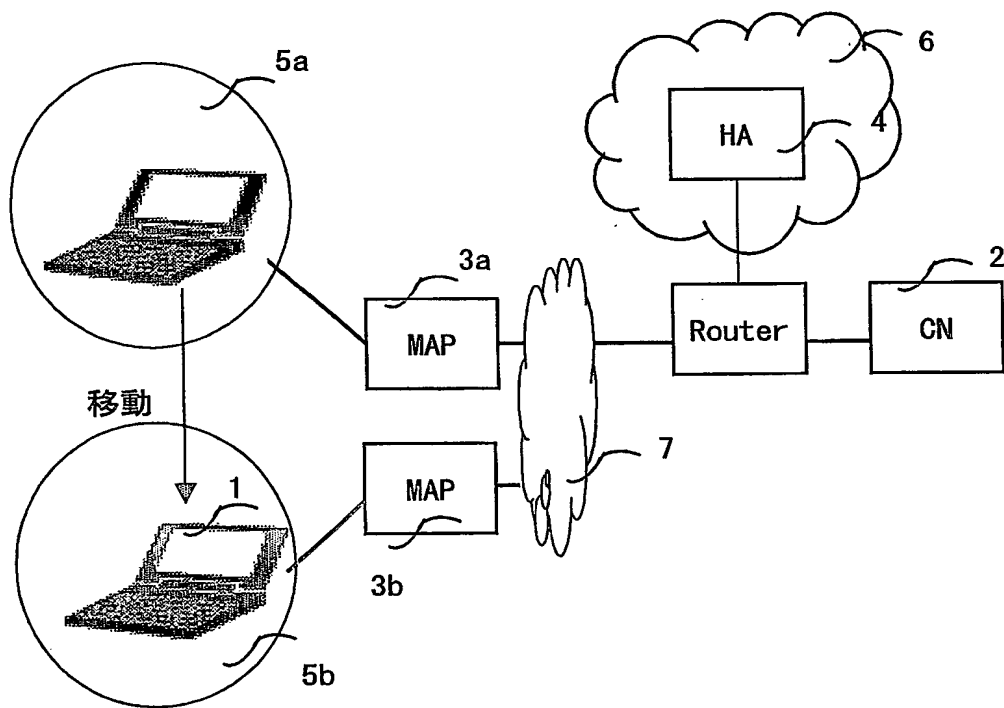


图26



27/39

図27



28/39

図28

端末機能ブロック図

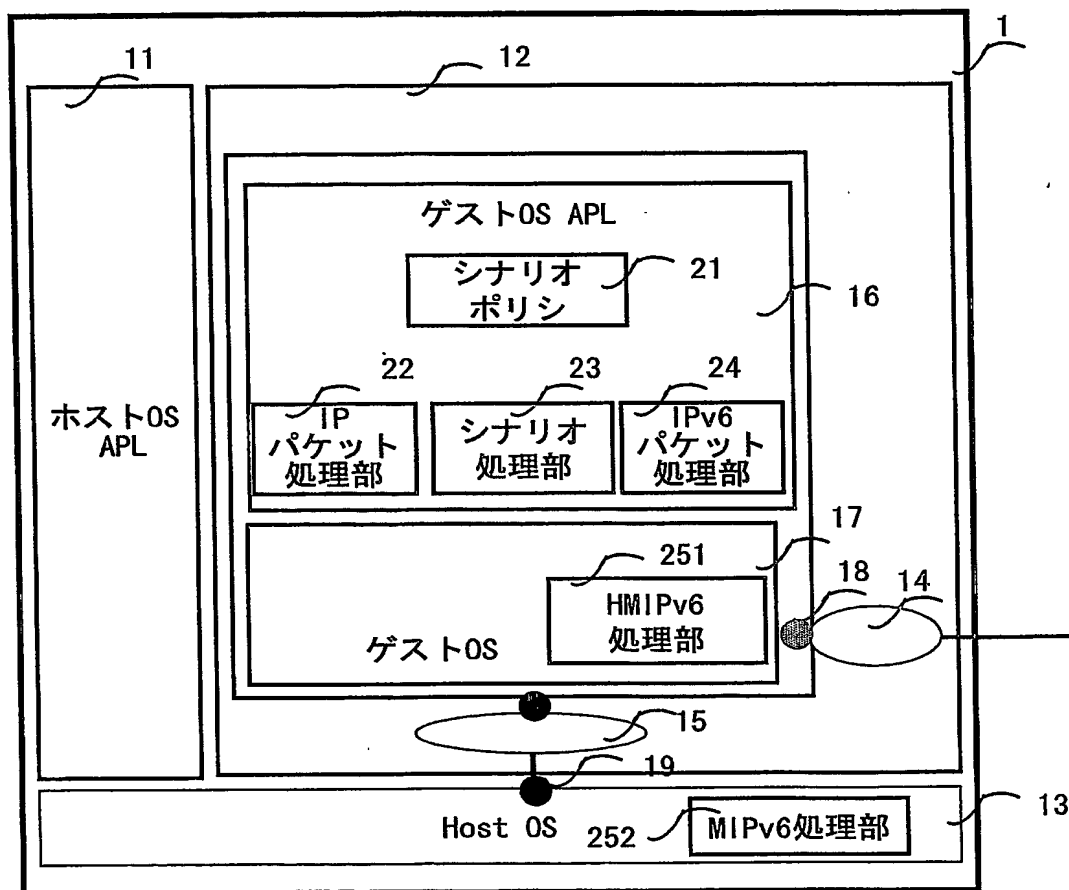
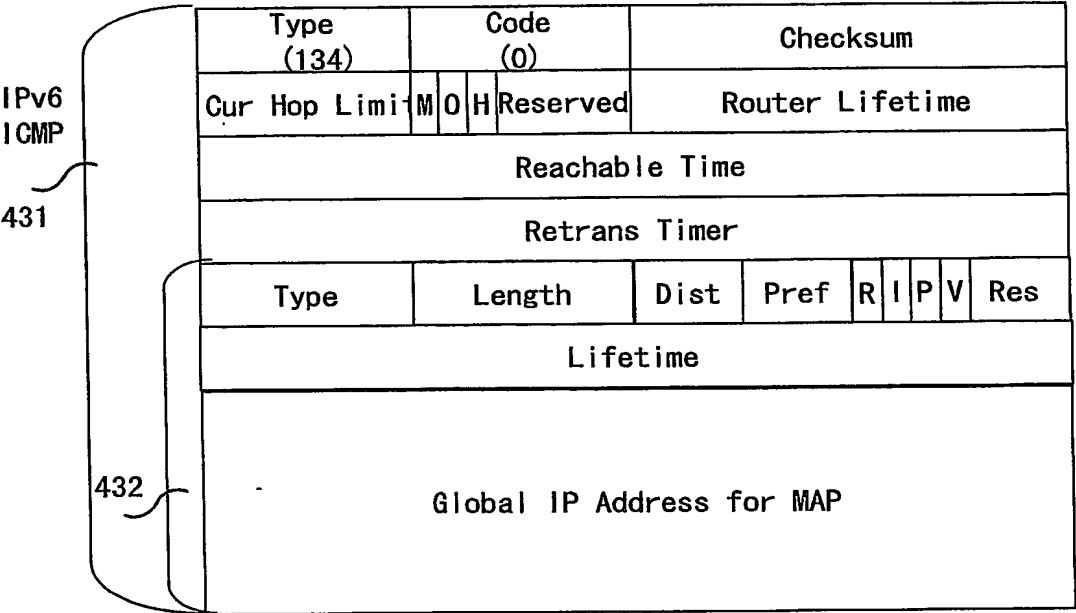


図29

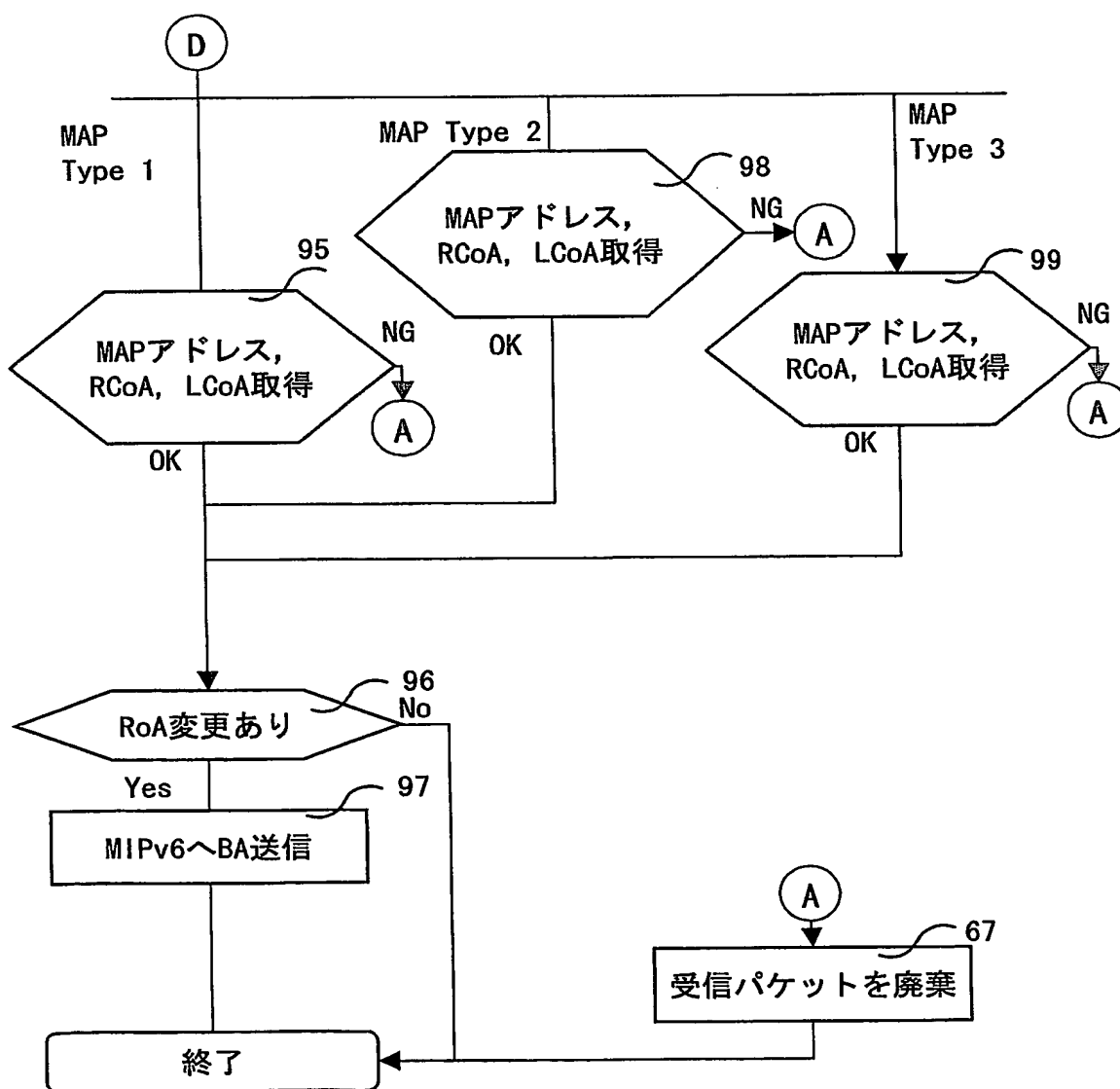
S4 Router Advertisementメッセージフォーマット



30/39

図30

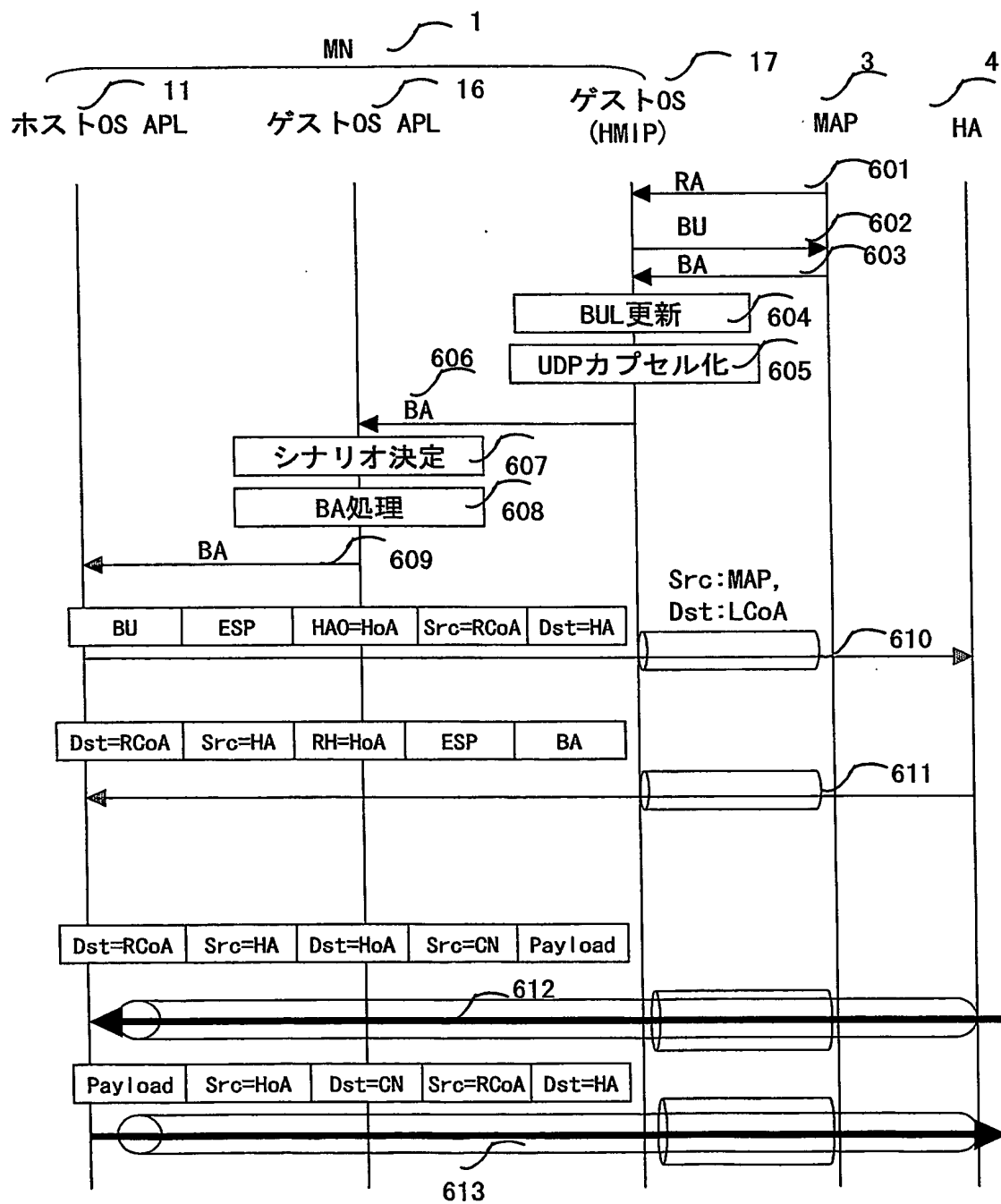
## 60 BA処理ルーチン



31/39

図31

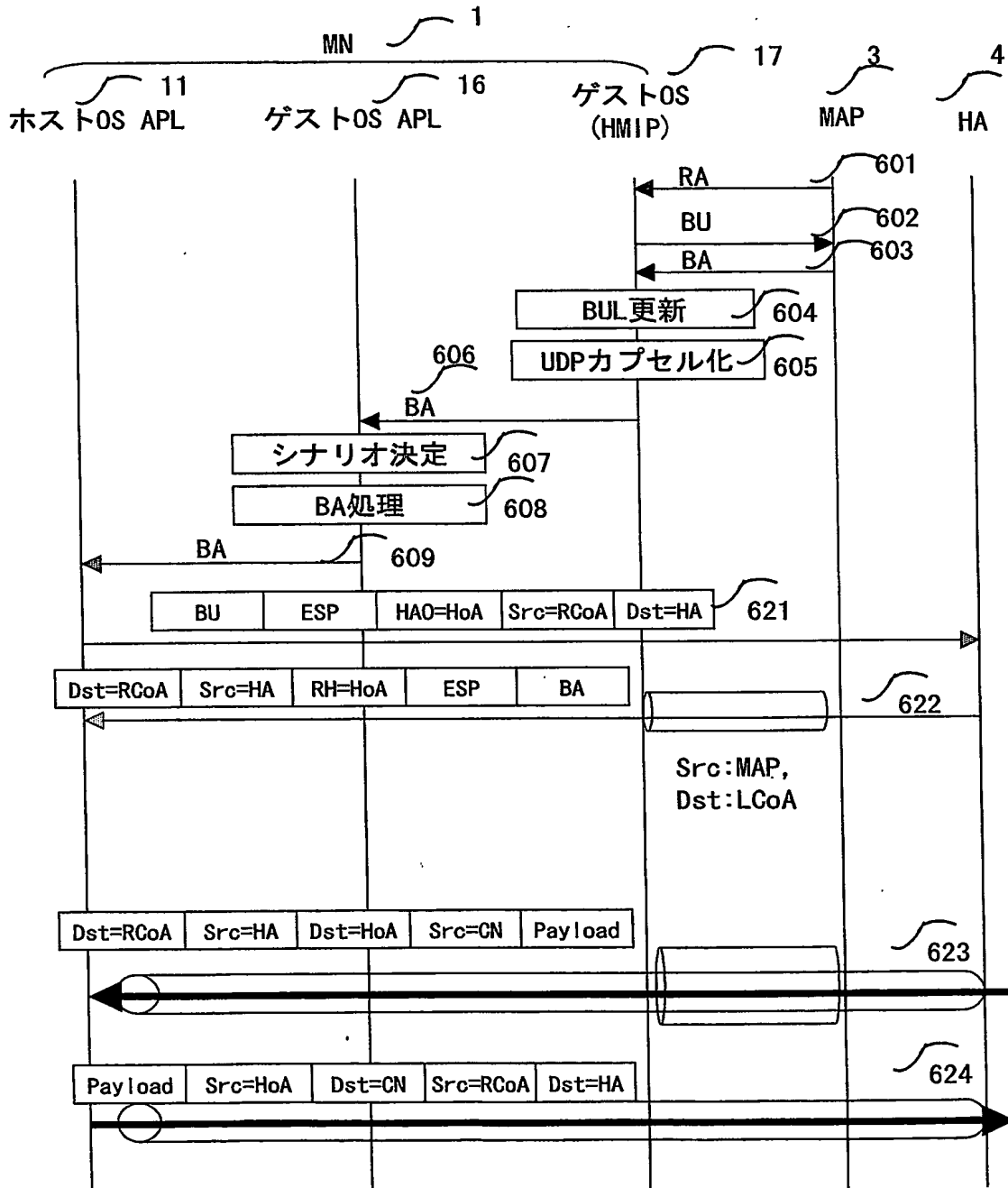
MAPタイプ1



32/39

図32

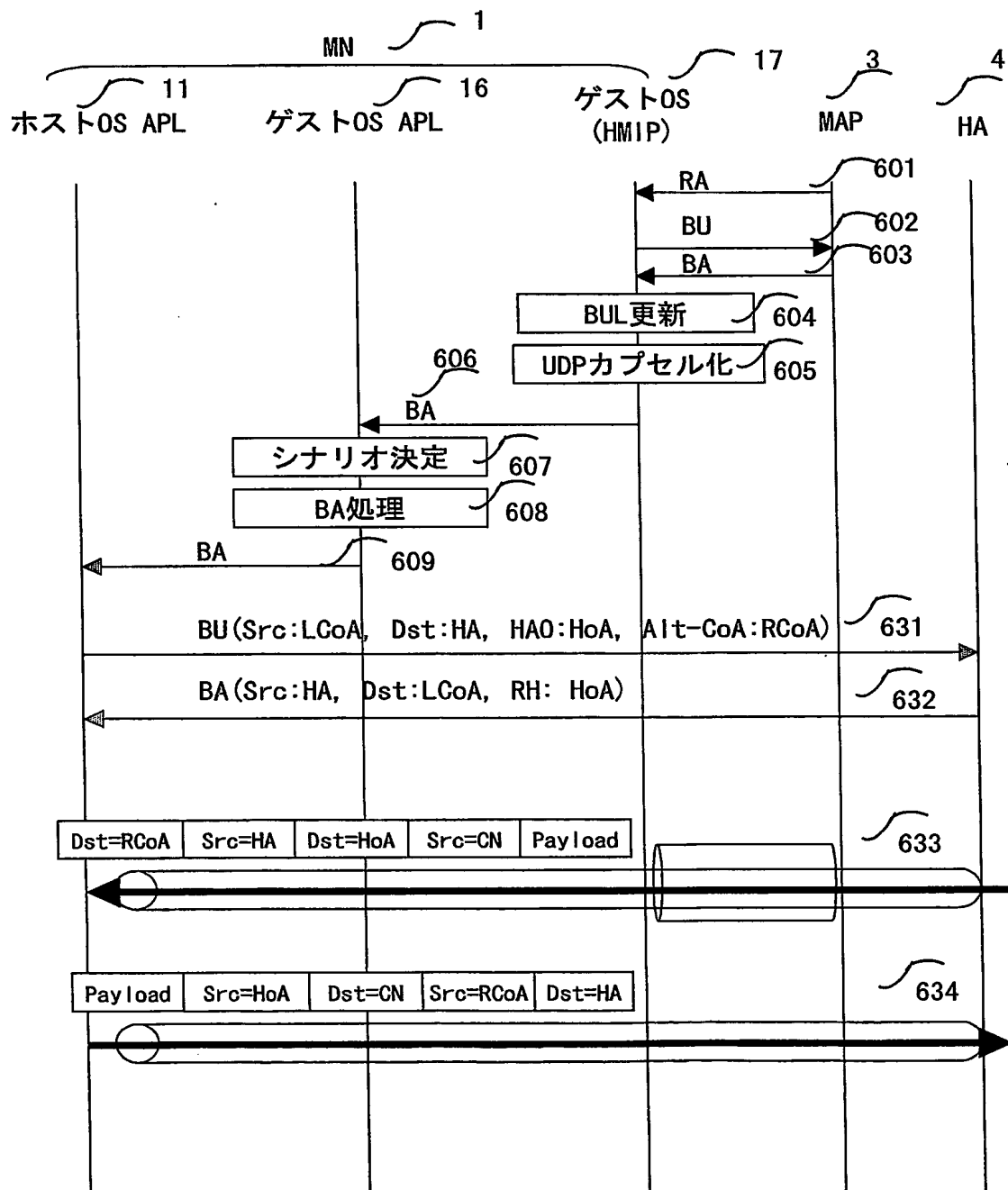
MAPタイプ2



33/39

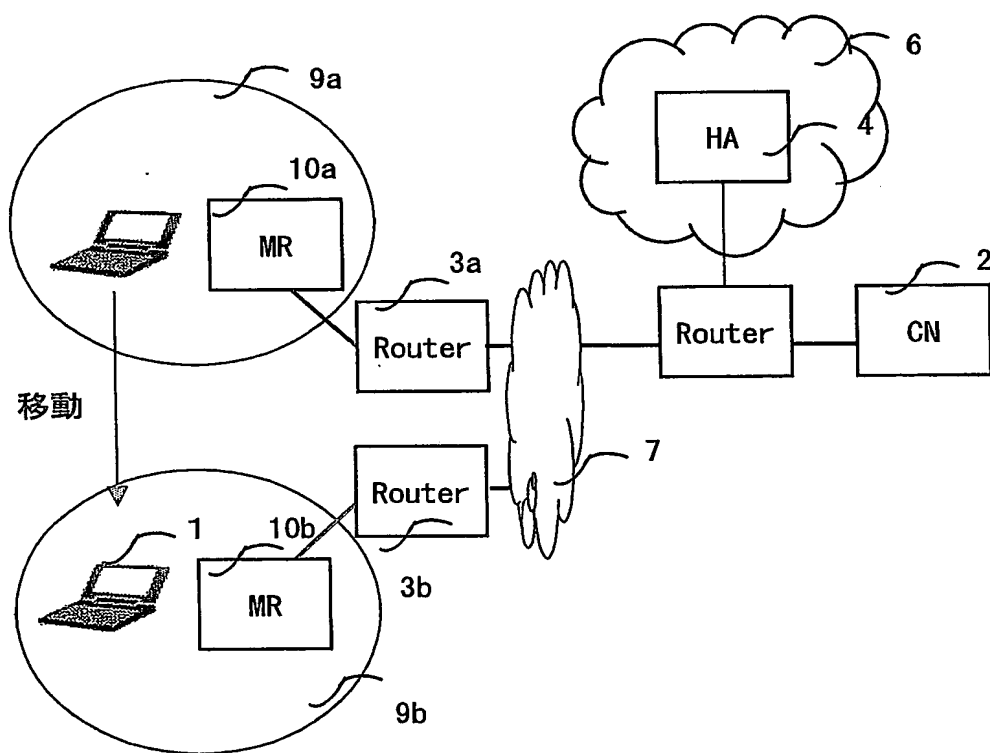
図33

MAPタイプ3



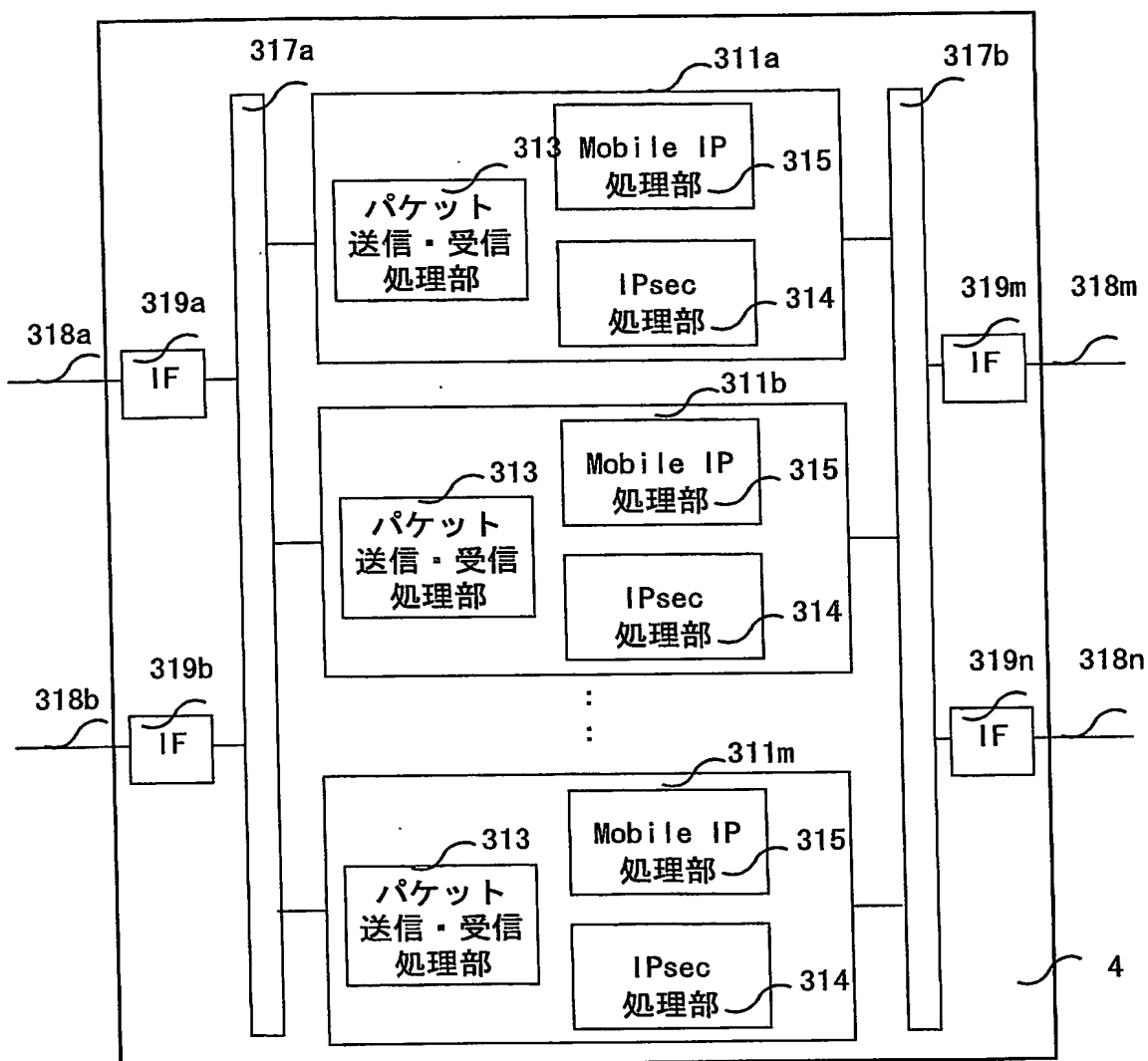
34/39

図34



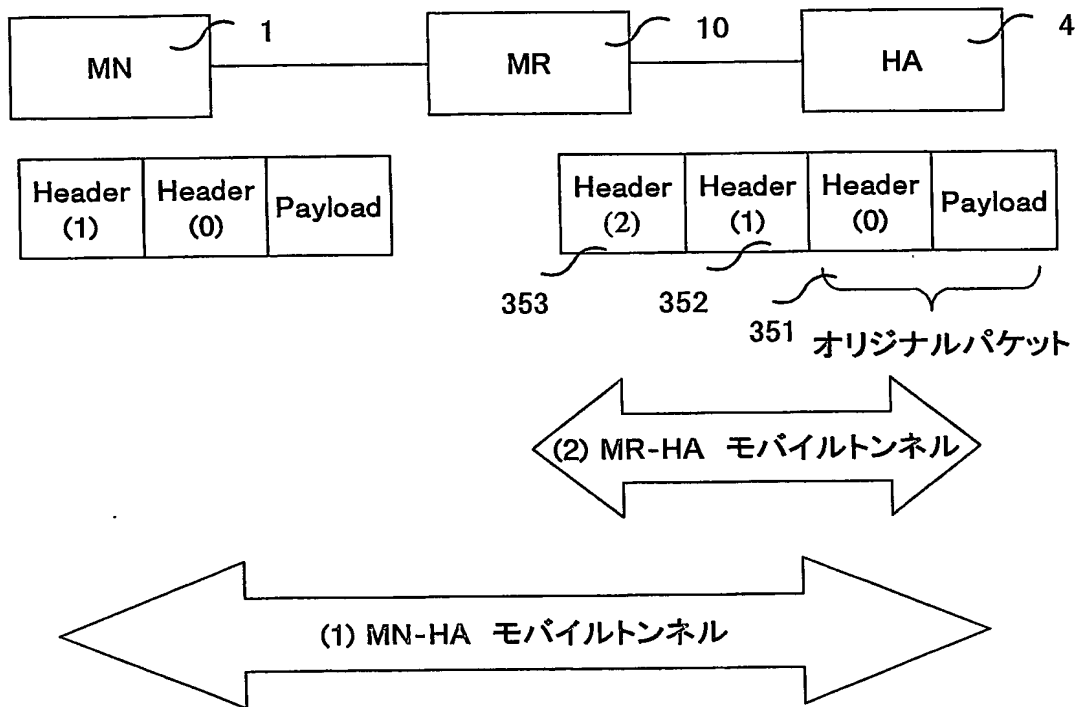
35/39

図35



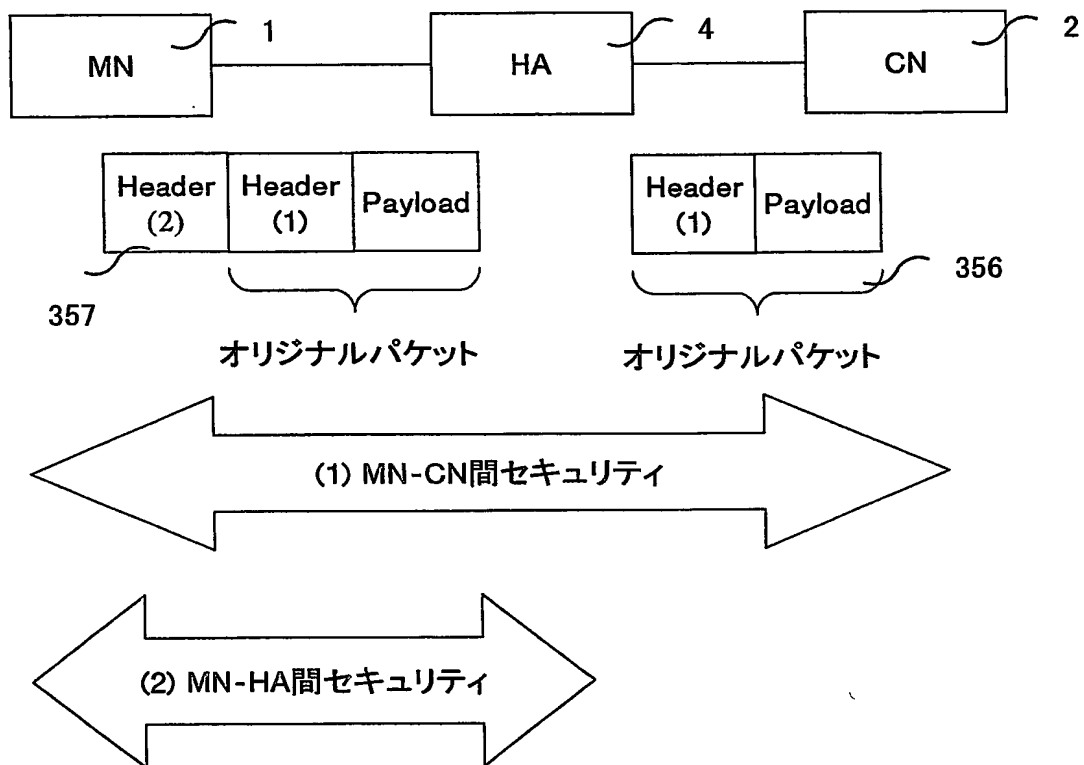
36/39

図36



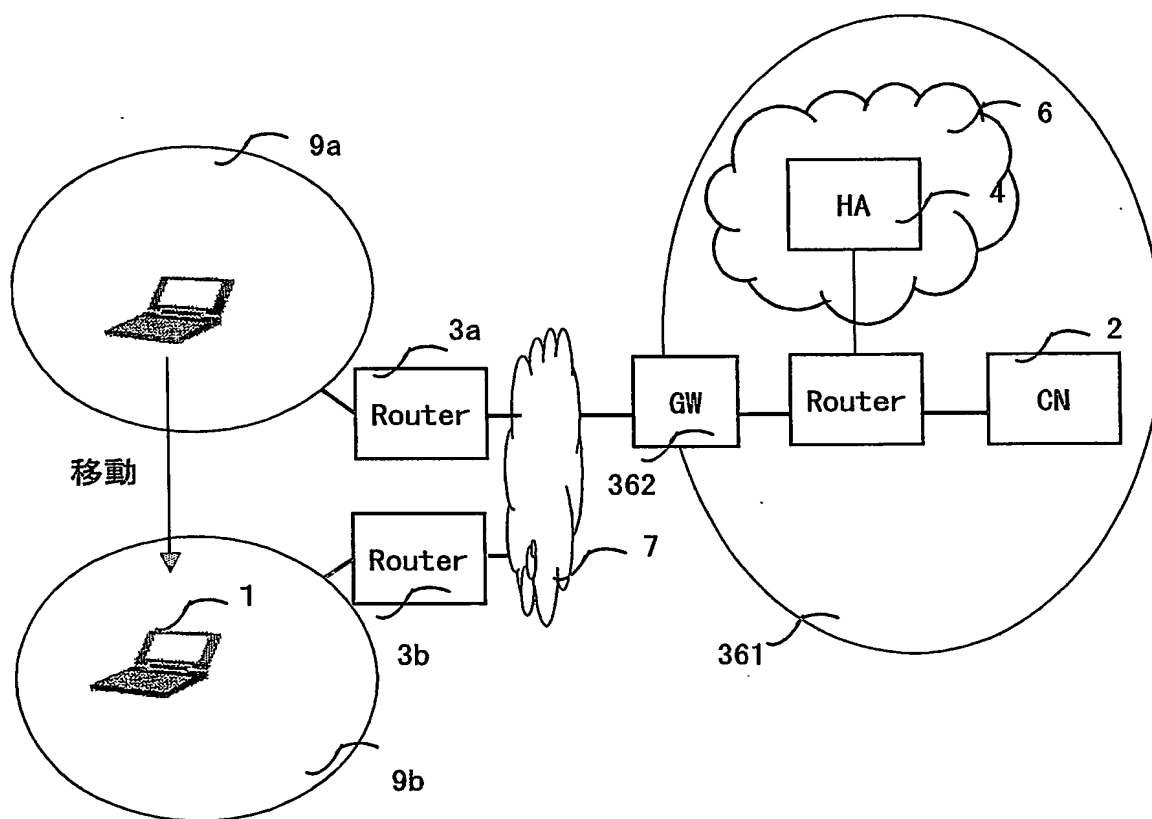
37/39

図37



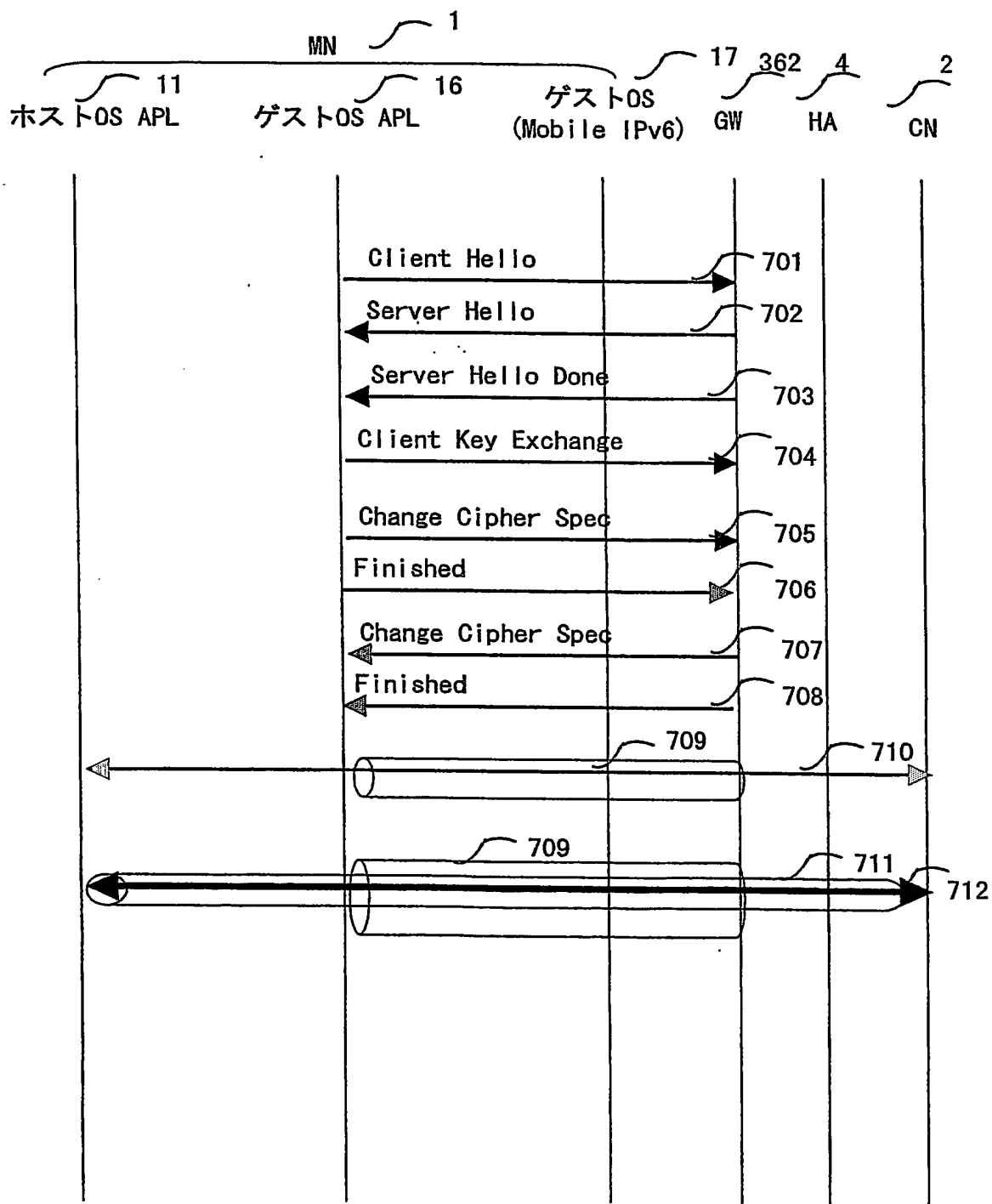
38/39

図38



39/39

図39



# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/010009

## A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl<sup>7</sup> H04L12/56

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)  
Int.Cl<sup>7</sup> H04L12/56

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched  
Jitsuyo Shinan Koho 1926-1996 Toroku Jitsuyo Shinan Koho 1994-2004  
Kokai Jitsuyo Shinan Koho 1971-2004 Jitsuyo Shinan Toroku Koho 1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2001-326697 A (Hitachi, Ltd.), 22 November, 2001 (22.11.01), Fig. 1 & EP 1156626 A2	1-28
A	JP 2002-185520 A (Fujitsu Ltd.), 28 June, 2002 (28.06.02), Fig. 1 & US 2002/0071417 A1	1-28
A	JP 2002-261806 A (Sony Corp.), 13 September, 2002 (13.09.02), Fig. 1 (Family: none)	1-28

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search  
25 October, 2004 (25.10.04)

Date of mailing of the international search report  
09 November, 2004 (09.11.04)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類 (国際特許分類 (IPC))  
Int. Cl.<sup>7</sup> H04L 12/56

B. 調査を行った分野  
調査を行った最小限資料 (国際特許分類 (IPC))  
Int. Cl.<sup>7</sup> H04L 12/56

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926-1996年  
日本国公開実用新案公報 1971-2004年  
日本国登録実用新案公報 1994-2004年  
日本国実用新案登録公報 1996-2004年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 2001-326697 A (株式会社日立製作所)、2001.11.22、図1 & EP 1156626 A2	1~28
A	JP 2002-185520 A (富士通株式会社)、2002.06.28、図1 & US 2002/0071417 A1	1~28
A	JP 2002-261806 A (ソニー株式会社)、2002.09.13、図1 (ファミリー無し)	1~28

☐ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

\* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの  
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの  
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)  
「O」 口頭による開示、使用、展示等に関する文献  
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの  
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの  
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの  
「&」 同一パテントファミリー文献

国際調査を完了した日  
25. 10. 2004

国際調査報告の発送日  
09.11.2004

国際調査機関の名称及びあて先  
日本国特許庁 (ISA/JP)  
郵便番号100-8915  
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)  
石井 研一

5K 8124

電話番号 03-3581-1101 内線 3555